РОЗДІЛ ІІІ

ПРИКЛАДНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАНКІВСЬКОЇ СИСТЕМИ ТА БАНКІВСЬКОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

Чиновник з портфелем вкраде набагато більше,
ніж тисяча гангстерів, озброєних автоматами
Дон Віто Карлеоне

Дослідивши і виклавши теоретичні та методологічні основи наукового дослідження та забезпечення національної, економічної, фінансової безпеки та безпеки банківської системи і банківської діяльності в Україні, а також правового механізму формування безпечного функціонування банківської системи України та управління нею, тепер час розглянути прикладні аспекти забезпечення безпеки банківської системи і банківської діяльності.

Адже класичний науковий пошук логічно повинен проводитися за схемою: від теоретичного узагальнення – через аналіз нормативно-правового регулювання досліджуваного процесу – до вивчення і узагальнення вітчизняної практики з урахуванням історіографії та зарубіжного досвіду. Лише такий методологічний підхід передбачає і забезпечує корисні для теорії й практики висновки та рекомендації, спроможні бажано впливати на досліджуваний об'єкт, досягти поставленої мети.

У пропонованому підрозділі розглядаються в логічній послідовності вузлові, найбільш важливі аспекти практичної діяльності банківської системи, що вирішальним чином впливають на стан і перспективи її діяльності та безпеки. Серед них, на наш погляд, серйозної уваги заслуговують такі гострі проблеми, як: внутрішні та зовнішні банківські ризики; «відмивання» коштів через банківську систему та його виявлення; банківська таємниця та її захист; запобігання використанню електронних і пластикових платіжних засобів в злочинних цілях; практика банківського менеджменту та роботи з персоналом банків і їх роль в забезпеченні безпеки банківської діяльності в Україні.

Приступимо до їх розгляду.

3.1. Внутрішні та зовнішні банківські ризики

У банківському бізнесі, як ніде, високий ступінь ризику, а тому управлінські помилки тут мають інколи непоправимі наслідки. Перманента криза вітчизняної банківської системи зумовлена, з одного боку, зовнішніми макроекономічними факторами, а з іншого – сильним впливом внутрішніх факторів, пов'язаних з діяльністю банків, які іменуються ризиками.

На теорію і практичне походження банківських ризиків існує чимало поглядів. На нашу думку, найповніше ця проблема опрацьована В.Т. Севруком [149], що і робить нас його прихильником. Згідно з його точкою зору банківський ризик –це певна ситуаційна характеристика діяльності будь-якого виробника, банку у тому числі, що показує невизначеність результату та можливих небажаних наслідків у разі невдачі. Такими наслідками, як правило, є: неотримання прибутку, виникнення збитків, внаслідок невиплат за отриманими кредитами тощо.

Рівень ризику зростає переважно за наявності таких умов:

– проблеми виникають раптом та несподівано;

– визначені нові завдання банку, що не відповідають минулому досвіду;

– керівництво не в змозі вживати потрібні та термінові заходи, що може призвести до фінансових збитків;

– наявний порядок діяльності банку чи недосконаліть законодавства заважає вжиттю деяких оптимальних для конкретної ситуації заходів.

Банківські ризики поділяються на види. Головним критерієм є час виникнення банківського ризику, тому за ним ризики розподіляються на ретроспективні, поточні та перспективні. За ступенем – низькі, помірні, повні. Але в процесі своєї діяльності банки зустрічаються з великою кількістю сукупностей ризиків.

Ми поділяємо думку, що за основними факторами виникнення банківські ризики можна поділити на політичні та економічні. При цьому під політичними ризиками слід розуміти ризики, що зумовлені змінами політичного становища, що негативно впливає на результати діяльності підприємств (воєнні дії на території держави, блокування кордонів, заборона на вивіз товару тощо).

Економічні ризики – це такі ризики, які зумовлені негативними змінами в економіці країни або самого банку. Найпоширенішим видом економічного ризику, в якому сконцентровані окремі ризики, є ризик незбалансованої ліквідності, становить неможливість своєчасно виконувати платіжні зобов'язання. До економічних ризиків можна також віднести зміни кон'юнктури ринку, рівня правління.

Слід зазначити, що ці види ризиків між собою тісно пов'язані і на практиці їх важко виокремити один від одного. В свою чергу, політичні й економічні ризики можуть бути зовнішніми та внутрішніми.

О.М. Ковалюк ризики у підприємницькій діяльності класифікує за характером їх походження, поділяючи на три види [102, с. 97]:

– виробничий ризик – це ризик, що може виникнути на виробництві і який слід враховувати під час складання прогнозів (пов'язаний з ризиком затримки у постачанні або недопостачанням матеріалів, сировини, палива, електроенергії, устаткування; чи постачанням їх гіршої якості; ризиком невиходу на роботу основних робітників тощо);

– комерційний ризик – це ризик, який треба враховувати під час визначення прогнозів, він може виникнути у процесі реалізації продукції (його потрібно відрізняти від норм природних втрат, які застосовують до певного виду товарів і продуктів, наприклад, норми вивітрювання сипких матеріалів, що застосовуються тільки тоді, коли компетентна комісія зафіксує відповідні втрати при транспортуванні);

– фінансовий ризик є найнебезпечнішим, його дуже важко спрогнозувати (це – передбачуване підвищення податкових ставок посеред фінансового року чи облікової кредитної ставки; певна фінансова стратегія фірми, якщо вона змінює ціни на цінні папери; зміна Національним банком курсу валют тощо).

Усі зазначені види ризику можуть бути трьох рівнів. Допустимим ризик є у разі, якщо підприємець після господарського обороту повернув собі витрати, однак не отримав прибутку. Це фактично показник порогу рентабельності.

Критичний ризик – це ризик, який треба враховувати в разі розрахунку прогнозів. У цій ситуації підприємець втрачає не тільки прибуток, а й частину витрат.

Катастрофічний ризик – це ситуація, коли фірма банкрутує [102, с. 97–98].

Згідно із системою В.Т. Севрука, до зовнішніх ризиків доцільно віднести ризики, що не пов'язані з діяльністю банка. На їх рівень впливає велика кількість факторів – політичні, економічні, демографічні, соціальні, географічні та ін.

До внутрішніх слід віднести ризики, що зумовлені діяльністю самого банку, його клієнтів чи конкретних контрагентів. На їх рівень впливає ділова активність керівництва банку, вибір політики та тактики тощо.

Останнім часом банки гостріше відчувають потребу в управлінні ризиками. Під управлінням ризиками слід розуміти всі вжиті заходи, які направлені на мінімізацію відповідного ризику та пошук оптимального співвідношення прибутковості й ризику, що має включати оцінку, прогноз і страхування відповідного ризику.

Загалом управління ризиками включає кілька етапів:

1) виникнення змісту ризиків, які виникають у зв'язку з певною діяльністю;

2) визначення джерел і обсягів інформації, потрібної для оцінки рівня ризику;

3) вибір критеріїв і методів для оцінки вірогідності реалізації ризику, побудова шкали ризиків;

4) вибір та розробка методу страхування ризику;

5) ретроспективний аналіз результатів управління ризиком, а також внесення коректив за попередніми пунктами схеми.

Тепер розглянемо зовнішні ризики докладніше.

До цього виду ризиків слід віднести країновий, валютний і ризик стихійних лих (форс-мажорні обставини).

Країновий ризик безпосередньо пов'язаний з інтернаціоналізацією діяльності банків та банківських установ, наявністю глобального ризику і таких, що залежать від політико-економічної стабільності країн-клієнтів та країн-контрагентів, імпортерів чи експортерів. Ця група ризиків актуальна для всіх банків заснованих за участю іноземного капіталу.

Спочатку оцінюють економічну ситуацію в країні, а потім обчислюють рівень сумарного ризику країни, використовуючи такі показники: приріст валового продукту; співвідношення розмірів інвестицій і валового доходу; ефективність інвестицій; середній рівень інфляції; зростання грошових надходжень; рівень реального внутрішнього кредиту; конкурентоспроможність економіки; торговельний баланс (експорт-імпорт); загальна зовнішня заборгованість; міжнародні резерви; вартість послуг щодо обслуговування зовнішньої заборгованості; розмір політичного ризику; рівень безробіття.

Щоб безпомилково визначити ризик певної країни, можна користуватися також і оцінками провідних країн, зробленими за окремими показниками. Вони, як правило, публікуються. Крім аналізу країни, слід зважати на ризики, пов'язані із зовнішньоекономічною діяльністю. Вони можуть бути зараховані як до зовнішніх, так і до внутрішніх ризиків банку, залежно від того, які рішення прийме менеджмент банку, а також конкретних обставин щодо його внутрішньої політики.

Валютний ризик пов'язаний із невизначністю майбутнього руху відсоткових ставок ціни національної валюти щодо іноземної. Він поділяється на економічний валютний ризик, ризик переводу і ризик угод. Перші спроби управління валютним ризиком були проведені на початку 70-х років, із введенням плаваючих курсів. Валютні курси, зі свого боку, структуруються таким чином:

1) комерційні, тобто пов'язані з небажанням чи неможливістю боржника (гаранта) розрахуватися за своїми зобов'язаннями;

2) конверсійні (наявні), тобто ризики валютних збитків у конкретних операціях. Ці ризики структуруються на ризики конкретних угод. Найпоширенішими методами зменшення конверсійних ризиків є:

– хеджування, тобто утворення компенсуючої валютної позиції для кожної ризикової угоди (відбувається компенсація одного валютного ризику – прибутків або збитків – іншим відповідним ризиком);

– валютний своп, що має два різновиди. Перший нагадує оформлення паралельних кредитів, коли дві сторони в двох різних країнах надають рівновеликі кредити з однаковими термінами і способами погашення, але виражені в різних валютах. Другий варіант – просто згода між двома банками щодо купівлі чи продажу валюти за ставкою «своп» і звернення угоди до попередньо визначеної дати (в майбутньому) за визначеною ставкою «своп». На відміну від паралельних кредитів свопи не включають платіж відсотків;

– взаємний залік ризиків за активом і пасивом, так званий метод «метчинг» (matching), в процесі якого віднімаючи надходження валюти від розміру її відтока, керівництво банку має можливість впливати на їх розмір;

3) трансляційні (бухгалтерські) ризики, що виникають під час переоцінки активів та пасивів балансів і рахунку «Прибутки і збитки» закордонних філіалів клієнтів, контрагентів. Ці ризики, в свою чергу, залежать від вибору валюти, перерахунку, її стійкості та низки інших факторів. Перерахунок може провадитися за методом трансляції (за поточним курсом на дату перерахунку) або за історичним методом (за курсом на дату проведення конкретної операції). Одні банки враховують всі поточні операції за поточним курсом, а довгострокові – за історичним, другі – аналізують рівень ризику фінансових операцій за поточним курсом, а деякі – за історичним; треті – обирають один із двох способів обліку та з його допомогою контролюють всю сукупність своїх ризикових операцій.

4) ризики форфетування, що виникають, коли форфетер (часто це банк) бере на себе всі ризики експортера без права регресу. Але водночас, форфетування (метод рефінансування комерційного ризику) має свої переваги, за допомогою яких може бути зменшений рівень ризику шляхом:

– спрощення балансових взаємовідносин можливих зобов'язань;

– покращання (хоча б тимчасово) стану ліквідності, що дає змогу подальшого зміцнення фінансової стійкості;

– зменшення вірогідності та можливості втрат шляхом страхування можливих ускладнень, яких майже не уникнути в період пред'явлення застрахованих раніше вимог;

– зменшення, чи навіть відсутність ризиків, пов'язаних з коливаннями процентних ставок;

– різкого зменшення рівня ризиків, пов'язаних з курсовими коливаннями валют і зі змінами фінансової стійкості боржника;

– відсутності ризиків і затрат, пов'язаних з діяльністю кредитних органів з відшкодування грошей за векселями та іншими платіжними документами.

І, нарешті, до зовнішніх ризиків відноситься ризик стихійних лих або, як ще їх називають, форс-мажорних обставин, який залежить як від наявності чи відсутності стихійних явищ природи і пов'язаних з ними наслідків, так і від різного роду обмежень з боку держави.

Зменшити вплив цих ризиків на діяльність банківської установи можна тільки шляхом своєчасного інформування один одного про зміни обставин.

На практиці найчастіше зустрічаються такі основні форми проведення зовнішньоекономічних операцій:

– пряма – прямий експорт-імпорт, здійснення зовнішньоекономічних зв'язків за допомогою різного виду посередників або дочірніх підприємств (банків) та філіалів, інвестиційні операції;

– побічна, що включає продаж і покупку ліцензії; виконання франчейзних операцій; укладання договору про технічне, управлінське обслуговування, придбання нових технологій і або «ноу-хау». Ці форми здійснення міжрегіональних і зовнішньоекономічних зв'язків рекомендуються для банків, що провадять свою діяльність за умови високого країнового, валютного (в своїй країні та країні партнера), кредитного, портфельного ризику.

Економічний валютний ризик – це ризик зміни вартості активів чи пасивів банків внаслідок майбутніх змін курсу. Аналізують економічний валютний ризик за допомогою таких показників: баланс банку; питома вага валютних кредитів, які виражені у національній валюті та видані за рахунок коштів, залучених у національній валюті; питома вага створених резервів за валютними кредитами, виражених у національній валюті, в обсязі загальних резервів банку на покриття збитків за кредитами; питома вага позитивної чи негативної курсової різниці в обсязі валютних операцій банку тощо.

Ризик переводу – це ризик зміни вартості активів і зобов'язань банку, пов'язаний зі зниженням курсу валюти. Потребує переоцінки активів і статутного капіталу банку, вираженого у валюті. Його аналізують та оцінюють за даними щодо руху вартості валют і прогнозів зміни курсу.

Ризик угоди зумовлюється невизначеністю вартості в національній валюті майбутньої угоди, укладеної в іноземній валюті. Щоб повністю оцінити цей вид ризику слід проаналізувати такі моменти:

– частку хеджування у конверсійних угодах, валютних свопів (рівновеликі кредити з однаковими строками, сумами і способами погашення, виражені в різних валютах у двох банках різних країн), угод «СПОТ»(купівля-продаж валюти в обумовлену на майбутнє дату за обумовленою ставкою);

– наявність і питому вагу взаємних заліків ризиків за активами і пасивами (визначають, віднімаючи суму валюти, яка надійшла, від усієї вивезеної валюти);

– частку великих валютних угод, динаміку операційних витрат за валютними операціями, швидкість розрахунків, обсяг угод між філіями, кількість застрахованих угод;

– збалансованість активів та зобов'язань банків за видами валют і строками; частку форвардних, ф'ючерсних, акційних операцій у зовнішньоекономічній діяльності банку.

Крім зазначених факторів, на валютний ризик банку впливає індекс ефективного валютного курсу.

Внутрішні ризики залежать від виду і специфіки банку, характеру його діяльності, тобто операцій, а також від складу його партнерів. Внутрішні ризики доцільно поділити на:

1. Ризики, які пов'язані з видом банку.

2. Ризики, пов'язані з характером банківських операцій: відсотковий ризик; портфельний ризик; ризик падіння загальноринкових цін; ризик інерції; транспортний ризик; лізинговий та факторинговий ризики.

3. Ризики, пов'язані зі специфікою клієнтури банку.

Діяльність універсального комерційного банку також універсальна, тобто вони займаються практично всіма видами банківських послуг (кредитними, розрахунковими та фінансовими). Зокрема, в останній час універсальні комерційні банки виконують дещо нетрадиційні операції, наприклад операції з різними видами цінних паперів, лізинг, факторинг, кліринг і т. ін.

Спеціалізовані комерційні банки в своїй діяльності орієнтуються в основному на надання конкретних послуг, тобто мають чітко виражену товарну орієнтацію, наприклад, інвестиційні, інноваційні, іпотечні, депозитні, клірингові та інші. послуги. Інші спеціалізуються на обслуговуванні визначених категорій клієнтів за галузевими (сільськогосподарські, будівничі, промислові) або функціональними (біржові, страхові, трастові) ознаками.

Також має місце так звана ринкова орієнтація ринків, тобто вони можуть бути регіональними, міжрегіональними, транснаціональними.

Вид і рівень внутрішніх ризиків, з якими стикаються різні види комерційних банків в основному залежать від специфіки їх діяльності.

У спеціалізованих комерційних банках, наприклад інноваційних, зустрічаються переважно ризики, пов'язані з кредитуванням нових технологій. Причини підвищення ризику можуть бути такі:

– використання нової технології розпочато дуже рано, ще до того, як затрати на виробництво були приведені у відповідність з реальним рівнем ринкових цін;

– продукція була випущена ще до того, як покупець був реально підготовлений платити за нововведення, тобто об'єм потенційного попиту дуже низький, щоб повернути витрати. Відповідно реальний попит ще нижчий за пропозицію;

– кількість постачальників і посередників, які були залучені перспективою росту пропозиції, завелика для конкретного ринку, що призвело до утримання конкретного банківського товару.

Разом з тим, більша кількість інвестиційних банків мають, наприклад, більш низький рівень портфельних ризиків, тому що в них є можливість пропонувати своїм клієнтам різноманітні послуги з управління кредитними портфелями цінних паперів. Таким чином вони отримують фінансові доходи.

У галузевих банках головне значення для рівня ризиків мають вид і специфіка конкретної галузі.

А діяльність універсальних банків наражається на ризики обох типів, а також на поєднані ризики.

Залежно від характеру банківських операцій ризики можна поділити на ризики активних і пасивних операцій.

Банк взагалі регулює свої ресурси для активних операцій завдяки пасивним. До пасивних операцій комерційних банків належать відрахування їх прибутку на формування та збільшення статутного капіталу; розміри кредитів, отриманих від інших юридичних осіб; депозитні операції. Взагалі лише перша група пасивних операцій формує власні кошти банку, а отримання банківських позик від інших юридичних осіб потрібне, найчастіше, для оперативного регулювання ліквідності балансів банку або для видачі непередбачених кредитів.

Депозитні операції – це операції по залученню коштів юридичних і/ або фізичних осіб у вклади або до запитання, або на визначений термін. Депозити можуть бути терміновими, до запитання, у вигляді заощаджених вкладів фізичних осіб, цінних паперів. Ризики пасивних операцій пов'язані з можливими ускладненнями в забезпеченні активних операцій ресурсами. Частіше за все – це ризик, пов'язаний з ефективністю діяльності визначального вкладника (один виробник або група «поріднених» компаній).

Ризики, пов'язані з депозитними операціями банку, можна поділити на такі види:

– ризик незбалансованої ліквідності. Він проявляється в масовому запитанні внесків клієнтами банку, включаючи масове дострокове відкликання коштів, із строкових і ощадних внесків, що може мати серйозні наслідки для банку, не виключаючи банкрутства;

– ризик втраченої вигоди за неможливості внаслідок різних причин об'єктивного і суб'єктивного характеру (наприклад, складна економічна ситуація на ринку, несприятлива кон'юнктура, конкуренція, відсутність партнерських зв'язків з іншими банками і т.ін.) залучити потрібні кошти в депозити для забезпечення його активних операцій (фактично є проявом ризику ліквідності);

– ризик трансформації, також проявляється у вигляді ризику ліквідності і відсоткового ризику.

Для попередження ризику з формування депозитів банкам слід дотримуватись оптимального співвідношення між пасивними і активними депозитними операціями, тобто вкладами підприємств в банк і вкладами, розміщеними одними банками в інших банках; визначати розмір і ліквідність залучених для зберігання цінних паперів для підвищення рівня та якості мобільних засобів; знайти доцільне мінімальне співвідношення власних засобів і ризикових активів; розробити методи розрахунку коефіцієнта пов'язання депозитів з обліком особливостей даного банку і керуватися ними при розміщенні депозитів.

Інформаційна база банку має відповідати певним вимогам, основними з яких є:

– побудова динамічних рядів окремих видів депозитних ресурсів;

– класифікація ресурсів за сумами, строками, групами клієнтів;

– визначення розміру стабільної частини за кожним видом депозиту;

– урахування номінальної та реальної ціни депозитних ресурсів (з урахуванням податків, норми обов'язкових резервів, тощо);

– визначення середньої ціни за групами депозитів та інше.

Після визначення основних ризиків у пасивних операціях і спираючись на інформаційну базу, депозитна політика банку повинна визначити методи, способи і засоби управління ризиками пасивних операцій.

Ризики активних операцій пов'язані з так званим рівнем відсоткового ризику, на який банки постійно наражаються в процесі своєї діяльності, тобто небезпека втрати внаслідок перевищення сплачених відсоткових ставок над отриманими. Підвищення відсоткових ставок призводить до падіння курсу цінних паперів із твердими процентами, а відтак – і до знецінення банківського портфеля, завдає курсових збитків. Крім того, різниця між відсотковими доходами і витратами становить основу банківського прибутку. Різка зміна ставок у різних сегментах ринку може негативно позначитися на прибутковості операцій банку.

Управління відсотковим ризиком складається з управління активами (кредитами і інвестиціями) та пасивами (залученими коштами).

Управління активами залежить від рівня ліквідності самого банку та портфеля його клієнтів із цінних паперів, а також від ступеня існуючої конкуренції, а управління пасивами – від доступності коштів для видачі позики.

Існує декілька концепцій управління відсотковими ризиками.

Портфельний ризик заключається в ймовірності втрат за окремими видами цінних паперів, а також у всій категорії позик. Портфельні ризики поділяються на фінансові, ризики ліквідності, систематичні та несистематичні.

Існують три основні концепції «теорії портфеля», а саме:

– концепція уникнення ризику, відповідно до якої акціонери та інвестори намагаються уникнути ризику завжди, коли це можливо. Ця концепція пов'язана із законом «спадаючої корисності», тобто чим більший капітал, тим менше акціонер намагається його збільшувати;

– незалежні інвестиції (портфелі інвестицій) або так звані «незалежні криві» становлять рівні корисності, за допомогою яких керівництво банківської установи координує рівень прибутку і ризиків;

– концепція «розподілу капіталу», яка може бути використана за наявності штучного обмеження інвестицій, в тому числі і з боку держави. У такому випадку банк (виробник, інвестор) не має можливості вкладати свої кошти в деякі проекти, навіть якщо він вважає їх виграшними. Найчастіше рівень портфельного ризику тісно пов'язаний з ризиком падіння загальноринкових цін.

Рівень відсоткового ризику залежить від:

– змін у портфелі (структурі) активів, включаючи співвідношення величин кредитів та інвестицій, активів з фіксованою і плаваючою ставкою, динаміки їх ціни на ринку;

– зміни в структурі пасивів, тобто співвідношення власних і залучених коштів;

– динаміки відсоткової ставки.

Для того щоб контролювати і управляти рівнем відсоткового ризику, розробляють конкретні стратегії діяльності банку залежно від конкретних ситуацій (див. табл. 4).

Таблиця 4

Способи управління рівнем процентного ризику

Ситуації	Рекомендації
1. Очікується зріст достатньо низьких відсоткових ставок	Збільшити терміни залучених коштів; скоротити кредити з фіксованою відсотковою ставкою; скоротити терміни інвестицій; продати частину інвестицій (у вигляді цінних паперів); отримати довгострокові займи; закрити деякі ризикові кредитні лінії
2. Відсоткові ставки зростають, очікується досягнення їх максимуму в найближчому майбутньому	Почати зменшення термінів залучених коштів; почати збільшення термінів інвестицій; почати підготовку до збільшення частки кредитів з фіксованою ставкою; підготуватися до збільшення долі інвестицій в цінних паперах; розглянути можливість дострокового погашення заборгованості з фіксованої відсоткової ставки
3. Очікується зменшення достатньо високих відсоткових ставок	Скоротити термін залучених коштів; збільшити частку кредитів з фіксованою ставкою; збільшити термін і розмір портфеля інвестицій; відкрити нові кредитні лінії
4. Відсоткові ставки зменшуються, наближуються до мінімуму	Почати збільшення терміну залучених коштів; почати скорочувати терміни інвестицій; збільшити питому вагу кредитів з плаваючою ставкою; скоротити інвестиції в цінних паперах; вибірково продавати активи з фіксованою ставкою або доходом

Аби зменшити ризик деякі банки вводять до відсоткової ставки за розміщеними коштами ризикову відсоткову ставку (договірну надбавку) або розмір страхового відсотку (коли позичку страхує сам банк). За умови інформації, як правило, аналізують реальні та номінальні відсотки. Щоб уникнути відсоткового ризику банки активно надають кошти на тривалі строки, а для рефінансування залучають кошти на менший термін.

Обчислюючи коефіцієнт відсоткового ризику, банки враховують ускладнення, які майже завжди виникають під час погодження строків платежу банку за зобов'язаннями і отримання платежів від клієнта; ймовірність невиконання зобов'язань партнером.

Чим вища відсоткова маржа банку, тим менший рівень відсоткового ризику. Іншими словами, маржа між відсотковими доходами від активів і відсотковими витратами за зобов'язаннями повинна бути позитивною.

Концепція «спред» – за якої аналізується різниця між зваженою середньою ставкою, що отримана за активами, і зваженою середньою ставкою, що виплачена за пасивами (зобов'язанням). Чим більша різниця

між цими двома величинами, тим рівень відсоткового ризику менший. Дані для аналізу беруться із статистичної звітності банку.

Концепція «розриву» полягає в аналізі незбалансованості активів і пасивів банку з фіксованою й плаваючою відсотковою ставкою. Береться перевищення суми активів з плаваючою відсотковою ставкою над пасивами з фіксованою відсотковою ставкою в статиці або за визначений період часу.

Фінансові ризики можуть бути визначені таким чином: чим більше залучених коштів мають банки, акціонерні товариства, підприємства, в тому числі і спільні банки, тим вищий ризик для їх акціонерів, засновників. Водночас, залучені кошти є важливим і вигідним джерелом фінансування, тому що найчастіше обходяться дешевше, ніж випуск та продаж додаткових тиражів цінних паперів.

Системний ризик пов'язаний зі змінами цін на акції, їх доходністю, поточним і очікуваним відсотком за облігаціями, очікуваним розміром дивіденду і додатковим прибутком, викликаним загальноринковими коливаннями. Він об'єднує ризик відсоткових ставок, ризик змін загальноринкових цін і ризик інфляції. Піддається достатньо точному прогнозу, адже тісний зв'язок (кореляція) між біржовим курсом акції і загальним станом ринку регулярно і достатньо достовірно реєструється різними біржовими індексами.

Несистемний ризик не залежить від стану ринку і є специфікою конкретного підприємства, банку. Він може бути галузевим і фінансовим. Основними факторами, що впливають на рівень несистемного портфельного ризику, є наявність альтернативних сфер докладання (вкладання) фінансових ресурсів, кон'юнктура товарних і фондових ринків тощо.

Сукупність системних та несистемних ризиків називають ризиком інвестицій.

Ризик падіння загальноринкових цін – це ризик недоотриманого доходу за будь-якими фінансовими активами. Найчастіше він пов'язаний з падінням цін на всі цінні папери, що обертаються на ринку одночасно.

Як правило, акції приватних фірм і акціонерних підприємств більш ризиковані ніж державні облігації. Але держава теоретично не може розоритися, тому що прибутки за її борговими зобов'язаннями гарантуються всім надбанням країни. Водночас, недержавні, акціонерні підприємства більш мобільні, ефективні, хоча і рівень банкрутства у них вищий.

Ризик інфляції – це ризик, який визначається життєвим циклом галузей. Основні фактори, які впливають на розвиток галузі, такі:

– переорієнтація економіки, що пов'язано із загальною економічно нестабільністю у світі, в окремих регіонах, країнах, ринках, ринкових сегментах, нішах і вікнах, з одного боку, і ростом цін на ресурси, з іншого;

– вичерпання будь-яких ресурсів;

– зміна попиту на внутрішньому і світовому ринках збуту.

Класифікація транспортних ризиків вперше була наведена Міжнародною торговою палатою в Парижі (1919 р.) і уніфікована в 1936 р., коли були оголошені перші правила ІНКОТЕРМС. Після останніх корекцій (2000 р.) різноманітні транспортні ризики класифікуються за ступенем відповідно в чотирьох групах E, F, C, і D.

Група E включає одну ситуацію, коли постачальник (продавець) тримає товар на своїх власних складах. Ризики бере на себе постачальник і його банк до моменту прийняття товару покупцем. Ризик транспортування від приміщень продавця до кінцевого пункту вже бере на себе покупець і його банк.

Група F включає три конкретні ситуації передавання відповідальності і ризиків:

– **FCA** – ризик і відповідальність продавця (і його банку) переносяться на покупця (посередника) в момент передавання товару в установленому місці;

– **FAS** – відповідальність і ризик за товар переходять від постачальника (і його банку) до покупця у відповідному (за договором) порту;

– **FOB** – продавець і його банк знімають з себе відповідальність після вивантаження товару з борту корабля.

Група C включає ситуації, коли експортер, продавець, його банк укладають з покупцем договір на транспортування, але не беруть на себе ніяких ризиків. Вони включають такі конкретні ситуації:

– **CFR** – продавець і його банк оплачують вартість транспортування до порту прибуття, але ризик та відповідальність за цілісність і збереження товару й додаткові затрати беруть на себе покупець і його банк. Перенос ризиків і відповідальності відбувається в момент завантаження корабля;

– **CIF** – крім зобов'язань, як у випадку CFR, продавець та його банк мають забезпечити і оплатити страховку ризиків під час транспортування;

– **CPT** – продавець і покупець (і їх банки) поділяють між собою ризики й відповідальність. У визначений момент (як правило, проміжний пункт транспортування) ризики повністю переходять від продавця та його банку до покупця і його банку;

– **CIP** – ризики переходять від продавця до покупця у визначеному проміжному пункті транспортування, але крім цього, продавець забезпечує і оплачує вартість страховки товару.

Остання група термінів D означає, що всі транспортні ризики покладаються на продавця. До цієї групи відносяться такі конкретні ситуації:

– **DAF** – продавець бере на себе ризики до визначеного державного кордону. Далі ризики бере на себе покупець і його банк;

– **DES** – передача ризиків продавцем покупцю проводиться на борту корабля;

– **DEQ** – передача ризиків проводиться в момент прибуття товару в порт завантаження;

– **DDU** – продавець бере на себе транспортні ризики за зіпсуття, втрати, розкрадання і т.ін. товару до визначеного договором місця (найчастіше це склад) на території покупця;

– **DDP** – продавець відповідальний за транспортні ризики до визначеного місця на території покупця, але останній їх оплачує.

Слід зазначити, що, якщо покупець не приймає товар з будь-яких причин або не має можливості оплатити в договірний строк, ризики можуть перейти до нього раніше.

Рівень банківських ризиків може виникнути також під час провадження лізингових і факторингових операцій, бартерних і клірингових угод.

Лізинг – це метод фінансування розвитку нової техніки й технології, розширення продажу обладнання, що особливо актуально за потреби прискореного впровадження окремих елементів реального основного капіталу, скорочення життєвого циклу товару тощо.

Для зменшення ризику лізингових угод слід розробити прискорені норми амортизаційних відрахувань або використовувати їх дострокове нарахування. Лізинг вважається на теперішній час операцією з підвищеним ризиком. Тому доцільно покриття збитків від нього провадити за рахунок резервного фонду банку.

Залежно від форми відношень між суб'єктами, що провадять лізингові операції, він може бути фінансовим, зворотнім, міжнародним. Кожен з перерахованих видів лізингу може бути прямим і побічним; строковим і поновленим (револьверним), чистим і повним.

Кліринг – це взаємна оплата між двома банками, районами, економічними одиницями, державами, під час якої проводиться обмін товарами без переведення грошей (валюти). Суть клірингу в наступному: за визначений календарний період, зазвичай один рік, суми взаємної торгівлі обертаються на конкретних банківських рахунках різних торгуючих країн на основі спеціального клірингового договору. Провадячи кліринг, кожна сторона-експортер отримує оплату за товар, що експортується, від свого банку. Банк, зі свого боку, не чекає переводу з банку-імпортера, а дебетує кліринговий рахунок і надсилає дебетове авізо відповідному банку, пов'язаному з імпортером.

Незважаючи на намагання виконання балансу під час взаємних поставок, найчастіше в кінці періоду одна сторона має перевагу, тобто авуар, на свою користь. Вона або не бажає більше товарів свого партнера, або їй потрібні гроші. Тоді ця сторона може продати свій авуар, зазвичай

за допомогою посередника, в третю країну. В такому випадку виникає різниця між вартістю клірингової валюти і вартістю конвертованої валюти. У цифровому вираженні цю різницю називають дизажио. Якщо, наприклад, 100 клірингових доларів обмінюють на 85 конвертованих, дизажио дорівнює 15%. Продаж клірингової валюти називається суітч (від англ. переключати). Цей термін зустрічається і у випадках, коли змінюють об'єкт і/ або суб'єкт торгових угод. Наприклад, під час продажу малоперспективних цінних паперів, зміни партнерів у випадку кредитних угод і т.ін.

Бартерні угоди – це форма компенсації, коли товар оплачується не грошима, а товарами. Бартерні угоди можуть бути міжфірмовими та міждержавними.

Найчастіше міжфірмові бартерні угоди здійснюються за допомогою різноманітних посередників.

Міжнародні бартерні угоди, так як і кліринг, пов'язані з прайс-листами, технічним кредитом, валютою для перерахунку вартості товарів, але вони не пов'язані з конкретним часовим періодом, і тривалість бартерних договорів залежить від якості та вартості товарів, вказаних у конкретних прайс-листах.

Для зменшення ризику у факторингових операціях слід аналізувати платоспроможність позичальників, вивчати характер їх господарських зв'язків з постачальниками, структуру платежів, конкурентноздатність продукції, кількість випадків її повернення тощо.

При покупці факторинговим відділом банку векселів у постачальників з'являється додатковий ризик придбання векселя, що не має покриття (бронзового). Цей ризик запобігається внесенням до договорів умов можливого їх розриву і припинення оплати рахунків та векселів при виникненні заборгованості факторинговому відділу більшої як 30 днів з моменту вичерпання терміну векселя. Частково компенсація цього ризику проводиться під час підвищення комісійної винагороди банку за подібні операції.

Одним з основних способів виміру рівня ризику є аналіз залежних і незалежних, зовнішніх та внутрішніх факторів, що впливають у конкретній ситуації за допомогою методів експертних оцінок.

Крім того, в практиці комерційних банків країн з розвинутою ринковою економікою широко використовується система банківських гарантій. Залежно від кількості банків, що беруть участь у гарантійних операціях, розрізняють прямі, побічні і посередницькі операції.

Зазвичай основними елементами банківських гарантій є сума, умови та строк виплати. Існують такі типи банківських гарантій:

1. Гарантії виконання договору або гарантії доставки. Їх надають підприємствам, які повинні провести доставку будь-якого товару,

забезпечити послугу або виконати інжинірингову роботу. Об'єктом гарантій є виконання договірних зобов'язань, в іншому випадку банк зобов'язаний виплатити визначену суму покупцю (споживачеві). Модифікацією цієї гарантії є гарантія рівня виконання, яка використовується тільки при виконанні будівельних, монтажних та інших конкретних інжинірингових робіт виробничого призначення. У цьому випадку банк зобов'язується виплатити певну суму при повному або частковому невиконанні договірних зобов'язань.

2. Гарантії торгу, які надаються учасникам торгів з метою забезпечення наявності прайс-листів, виконання взятих на себе зобов'язань. У випадку невиконання умов торгів банк також повинен виплатити певну суму потерпілій стороні.

3. Гарантії авансу при виконанні великих замовлень: побудові. Через те, що замовлення виконується протягом тривалого періоду часу, виконавець має бути впевненим, що після закінчення роботи споживач не передумає і не відмовиться провести оплату. Зі свого боку споживач має бути впевненим, що отримає замовлений товар у потрібній кількості та якості точно в строк. При невиконанні зобов'язань банк повинен виплатити певну суму потерпілій стороні. Іноді сума гарантій автоматично зменшується по мірі виконання деяких етапів зобов'язання.

4. Гарантія відсутнього коносамента передбачає тимчасове неспівпадання між транспортуванням товарів і пересилкою супровідних документів. З її допомогою знижується оплата за зняття додаткових складських приміщень, оплата за простої транспортних засобів, зменшується ризик від доставки неякісного товару, товару, що не відповідає всім раніше обумовленим вимогам і т.ін.

5. Гарантія неповної (некоректно складеної) документації. Банк забезпечує споживача і/ або виробника потрібними засобами для нормального продовження діяльності незалежно від конкретної несприятливої ситуації, пов'язаної з неправильним оформленням супровідної документації.

6. Гарантія для митних влад виражається в зобов'язаннях банків виплатити всі митні формальності, пов'язані з перевезенням товару.

По своїй суті банк – це комерційне підприємство. Основними принципами взаємовідносин «банк-клієнт» є принцип отримання прибутку банком при мінімальних затратах і принцип мінімізації всіх видів ризиків. Банк насправді може ризикувати (і він ризикує щоденно в процесі своєї діяльності) своїм власним капіталом, але не капіталом клієнта, його прибутком.

З метою мінімізації ризику банк повинен:

– диверсифікувати портфель своїх клієнтів, що веде до диверсифікації всіх видів ризику, тобто його розрідження;

– намагатися надавати кредити у вигляді менших сум більшій кількості клієнтів;

– надавати більші суми клієнтам на консорційній основі і т.ін.

Розглянемо один із способів класифікації клієнтів банку, за допомогою якої може бути зменшений рівень всіх видів банківського ризику.

Згідно із теорією ризиків основною ознакою належності підприємства до тієї чи іншої галузі є призначення продукції, що випускається. Розрізняють підприємства первинної сфери, до якої відносяться сільськогосподарські підприємства; підприємства вторинної сфери (промислові), які зі свого боку, можуть бути добувними та переробними; і, нарешті, підприємства третинної сфери, що надають різного виду послуги (банки, страхові, аудиторські, консультативні компанії і т.ін.) і провадять свою діяльність в сфері збуту (оптового або роздрібного).

Для зменшення рівня галузевого ризику банку слід обслуговувати клієнтів, що належать до різних галузей народного господарства. Таким чином, зменшується рівень ризику сезонності, тому що верхні та нижні точки сезонних коливань (традиційні й неочікувані) різноманітних клієнтів не співпадають, ризику інфляції, валютних ризиків, ризиків форс-мажорних обставин.

Галузевий ризик пов'язаний з економічною і фінансовою динамікою самої галузі. Чим галузь динамічніша, тим вищий ступінь ризику.

Фактори, що впливають на рівень галузевого ризику, можуть бути згруповані таким чином:

– діяльність альтернативних галузей за певний період часу. Аналіз проводиться за допомогою специфічного аналізу рівня середньоквадратичних відхилень;

– внутрішньогалузева конкуренція, яка може бути ціновою й неціновою і залежить від складності входження нових виробників у галузь, наявності або відсутності товарів-замінників, ринкової сили покупця (споживача), рейтингу постачальників і посередників, авторитету доброчинних контактних аудиторій.

Одним із основних способів виміру рівня галузевого ризику є отримання коефіцієнта галузі (бета-коефіцієнта). Цей коефіцієнт визначає рівень коливань або відхилень результатів діяльності конкретної галузі у відношенні до результатів діяльності всієї економіки ринку країни. Очевидно, що для аналізу рівня галузевого ризику потрібна достатньо поширена база даних макроекономічних показників за достатньо великий період часу.

Галузь з показником коефіцієнта вищим за одиницю має більш високий рівень ризику, ніж галузь, з показником коефіцієнта меншим за одиницю. Зазвичай цей аналіз проводиться за допомогою регресійних моделей або методів факторного аналізу.

Крім цього, рівень галузевого ризику достатньо динамічний, і слід провадити аналіз цього рівня не тільки в статиці, але і в динаміці.

Залежно від розмірів підприємств клієнти поділяються на три групи – дрібні, середні та великі.

Дрібні та середні позичальники більш гнучкі, швидше можуть відреагувати на потреби клієнтів, ринку. Їх структура більш легка, що дає їм можливість швидше змінювати напрям своєї ділової активності, отримати високий прибуток.

Але дрібні та середні підприємства зазвичайно мають невеликий власний капітал, що призводить до банкрутства за умов жорсткої конкуренції, будь-яких непередбачених змін політичного та економічного характеру (ризик форс-мажорних обставин). Часто вони мають невелику кількість клієнтів, контролюють невеликі ринкові сегменти. Тому кількість банкрутств більша для невеликих і середніх підприємств.

Великі підприємства, навпаки, більш інертні. Вони не реагують швидко на зміни в потребах ринку та конкретного клієнта, не часто змінюють напрям своєї ділової активності, але мають вагомий власний капітал і можуть «пережити» деякі несприятливі економічні ситуації. Такі підприємства мають можливість провадити всі види гарантійного і післягарантійного обслуговування, витрачати більше коштів на різного роду рекламу. Іншими словами, вони майже завжди забезпечують середній прибуток і рентабельність. Такі підприємства мають можливість створювати дочірні фірми, філіали, розширювати свій ринок, перетворити його в міжнародний.

За належністю до різних видів власності виробники можуть бути розділені на такі групи – державні, приватні, кооперативні, акціонерні. Останні два види можуть бути спільними (транснаціональними) і мононаціональними. Залежно від цього різні види ризиків набувають більшої чи меншої значущості в процесі їх діяльності. Завданням банку є підібрати портфель своїх клієнтів таким чином, щоб самому мати оптимальне співвідношення між активними і пасивними операціями, зберігати достатній рівень своєї ліквідності та рентабельності.

Для цього слід проводити регулярний аналіз рівня всіх видів ризиків, визначати їх оптимальне значення для кожного конкретного моменту і використовувати весь набір способів управляти ними.

І, нарешті, можна зазначити ще кілька способів управління рівнем ризику діяльності банків і банківських установ. До них можна віднести:

– попередню оцінку ймовірних втрат за допомогою прогнозних методів аналізу статистичної і динамічної достовірної інформації про діяльність самих банків, їх клієнтів, контрагентів, їх постачальників і посередників, конкурентів та різних груп контактних аудиторій. Для цього

комерційним банкам потрібно створити відділи, що мають займаютися аналізом ризиків і виробляти заходи з управління ними в системі маркетингу;

– динаміку відсоткових ставок, які за збільшення ступеня ризику збільшуються, і навпаки, тобто ставки за вільно утвореними інструментами менші ставок за інструментами з обмеженою оборотністю, ставки у пасивних операціях і операціях на міжбанківському ринку зазвичай менші ставок у активних операціях і кредитних операціях з клієнтурою; чим стабільніший позичальник, тим менші відсоткові ставки; довгострокові змінюються більш плавно, ніж короткотермінові; ставки за кредитами із забезпеченням і короткотермінових операціях менші, ніж ставки без забезпечення і за короткотермінових операцій;

– страхування кредиту, як гарантії на випадок несприятливих обставин;

– хеджування (страхування ризику);

– відмову від пропозицій позичальника за досить великого ризику;

– розрахунок умов кредиту, що застосовується переважно у випадках невеликих позик і особистого кредитування;

– диверсифікацію ризику, тобто розосередження. Вона може проявлятися в різних видах:

а) надання кредитів дрібними сумами більшій кількості клієнтів за збереження загального обсягу кредитування;

б) надання кредитів на консорційній основі, коли для видачі великої суми кредиту об'єднуються кілька банків, утворюючи консорціум;

в) залучення депозитних вкладів, цінних паперів у невеликих розмірах, але від більшої кількості вкладників;

г) отримання достатнього забезпечення за виданими кредитами. Важливими умовами реалізації цієї умови є наявність заставного права; вміння правильно аналізувати й оцінювати платоспроможність позичальників; правильна орієнтація з оперативного відшкодування боргу; застосування системи нормативів у активних і пасивних операціях. Вони встановлюються центральним банком і обов'язкові для виконання.

Регулювання банківського ризику базується не на оцінці фінансового положення позичальника, а на встановленні певного співвідношення між сумами виданих кредитів і власних коштів самого банку, тобто передбачається створення резервного потенціалу у банків для покриття ймовірних збитків у випадку розорення клієнтів.

Тільки від конкретної ситуації залежить, яким способом комерційні банки будуть аналізувати рівні всіх своїх ризиків і управляти ними.

Як відомо, головний біль багатьох банків в Україні – неплатоспроможні позичальники. Тим часом у структурі кредитних ринків розвинутих країн

активно діє так звана «шестерня», система спеціалізованих кредитних бюро, які відіграють важливу роль у зменшенні ризиків угод, що провадяться.

Вивчення світового досвіду [124, с. 28] показало, що вони створюються для того, щоб кредитор міг одержати інформацію про стан платоспроможності позичальників, порушення ними платіжної дисципліни і на її підставі оцінити ступінь ризику майбутньої угоди. Закордонний досвід показує, що розв'язати ці проблеми можна тільки за допомогою кредитних бюро, створених для обміну відомостями про прохачів позик між кредиторами. Це, з одного боку, зменшує ризики угод, що провадяться, а з іншого – змушує всіх учасників ринку вкрай вимогливо ставитися до своєї кредитної історії, яка фактично є основою ділової репутації.

В основі організації і функціонування кредитних бюро закладена сучасна інформаційна система, що забезпечує збір, обробку і поширення інформаційних даних про юридичних і фізичних осіб – одержувачів кредитів. Кредитне бюро, де на кожного позичальника формується спеціальна картотека, забезпечує максимальну безпеку інформації, допуск до якої обмежений.

Сьогодні кредитні бюро в тій або іншій формі діють у багатьох державах світу. Вперше цей регулятор кредитного ринку виник ще у 1860 р. в Австрії. У 1890 році кредитні бюро було створено у США і Швеції. Пізніше їх заснували у Фінляндії (1900), ПАР (1901), Канаді (1919), Німеччині (1927), Аргентині (1950), Великій Британії (1960), Японії (1965) та в інших країнах.

У США добре відомі три великі кредитні бюро – Equifax, Experian і Trans Union, які є приватними підприємствами, що функціонують для одержання прибутку від своїх інформаційних послуг. Їх обороти з надання так званих кредитних історій становили донедавна близько 1,5 млрд дол. У більшості європейських країн і Японії кредитні бюро створюються у формі приватних компаній, що належать консорціуму кредиторів.

У Фінляндії і Бельгії такі бюро керуються або ліцензуються урядовими агентствами. Діюче в Німеччині кредитне бюро є об'єднанням восьми регіональних, у правовому й економічному відношенні самостійних товариств – Товариство захисту у справах загального забезпечення кредитів (SCHUFA).

З 2000 р. діє НП «Національне кредитне бюро» у Російській Федерації, засновники якого – Торгово-промислова палата Росії, Держкомстат і корпорація Dun & Brandstreet (мережа, що розвиває кредитні бюро в усьому світі). Крім або замість кредитних бюро в багатьох країнах організовано установи державної реєстрації кредитів – Public credit registers (PCR). Тобто, інститут кредитних історій досить швидко розвивається, і не останню роль у цьому відіграє ініціатива самих кредитних установ.

Щомісяця всі кредитори (банки, фінансові компанії, компанії-емітенти кредитних карт, інвестиційні компанії, торгові компанії, що надають комерційні кредити) направляють у кредитне бюро дані про стан кредитних рахунків своїх клієнтів. До бази даних кредитного бюро вводяться всі легальні повідомлення про кредитні операції, банкрутства, судові процеси, податкові пільги тощо.

У США робота кредитних бюро регулюється законом про достовірну оцінку кредитоспроможності, прийнятим 1971 р.

Поширення інформації провадиться за певну плату відповідно до запитів кредитних установ, яким за лічені секунди надсилається відповідь з даними про потенційного клієнта. Отримана інформація використовується всіма постачальниками кредитів – банками, фінансовими установами, кредитними товариствами тощо – під час прийняття рішень про надання кредиту тій чи іншій особі.

У деяких країнах (наприклад, в Індонезії, Китаї) поширення інформації про кредити, видані приватним особам, або заборонено, або обмежено. Головні причини цього – не тільки законодавчі обмеження, а й небажання кредитних установ із міркувань конкуренції поширювати позитивні дані про своїх клієнтів.

«Результати проведеного фірмою Fair Isaak аналізу показали, що якби кредитні установи задовольняли всі запити фізичних осіб на кредити, то 12,8% усіх кредитів протягом року були б «поганими», тобто погашалися б невчасно або не погашалися б зовсім. Якби кредитні установи брали до уваги тільки «позитивні» досьє, то вони задовольняли б 81% заявок на одержання кредитів. При цьому частка сумнівних кредитів становила б 4 %. А якщо враховувати поряд із «позитивними» і «негативні» досьє, то частка поганих кредитів зменшиться до 3,1%. Отже, під час прийняття рішень про кредитування фізичних осіб важливо спиратися на базу даних, що містить і позитивні, і негативні відомості про потенційних позичальників» [124, с. 28]

Незважаючи на всю специфічність українських умов, закордонний досвід розвитку кредитних бюро корисний для нашої країни. Сьогодні створенню в нас таких структур перешкоджає відсутність спеціального закону про кредитні бюро. Якщо названий закон буде розроблено і прийнято, в результаті чого це бюро у нас з'явиться, то кредитні ризики можуть бути значно зменшені. Як заявив голова НБУ Сергій Тігіпко, Національний банк готовий узяти на себе функцію зі збору і збереження інформації про позичальників. Отже, справа за практичною реалізацією.

У практичній площині політичні й економічні ризики сьогодні диктують БСУ свої правила.

Закордонні аналітичні центри постійно відстежують розвиток подій в Україні і дають відповідні рекомендації своїм банкам. Наочним в цьому відношенні є звіт міжнародного рейтингового агентства Fitch. «Україна: після виборів», опублікований за підсумками березневих (2002 р.) виборів до Верховної Ради України. Проаналізувавши та оцінивши розстановку політичних сил в Україні після виборів, агентство робить невтішний висновок: «... через те, що опозиція планує вересневі акції протесту і загрожує розпочати процедуру імпічменту нині діючого Президента, ***політичні ризики в Україні значно зростуть.*** А це в світлі наростаючих обертів Президентської кампанії, гарантує збереження в Україні політичної нестабільності і, як наслідок, ***погіршення становища в економіці країни…*** (виділено авт.)» [124, с. 4].

При цьому агентство, заявивши про слабкість української економіки, високий рівень корупції, низьку капіталізацію банківської системи, викликало у західних «компаньйонів» сигнал тривоги. Після цього мали місце відмови Україні у кредитах з боку Міжнародного валютного фонду та інших кредиторів.

Як висловився у квітні 2003 р. С.Тігіпко: «ризик економічного зростання полягає, зокрема, і в політичних процесах. А отже, ми неминуче зіштовхуємось із серйозними перешкодами банківського реформування.

Україна впритул підійшла до проведення політичних реформ... Нашій державі, суспільству, яке лише на шляху до громадянського, вкрай необхідно структурувати політичну владу, чітко розподілити повноваження владних інституцій.

Розумію – цей процес складний і неоднозначний. Тому потрібні неабиякі зусилля і добра воля політиків, громадських організацій, щоб гідно завершити вкрай необхідну справу» [159, С.8].

Сьогодні вирішується доля парламентсько-президентської або іншої моделі держави, коли необхідно надати більшої ваги Верховній Раді, представницьким органам. Розширюючи повноваження парламенту, слід дотримуватись балансу політичних сил.

Іншого статусу – економічної влади в державі – має набути уряд на основі принципу формування коаліційного уряду.

«Це внутрішні проблеми, з якими пов'язані і відповідні ризики економічного зростання, функціонування економічних та фінансових інститутів. Послаблення політичного протистояння, зрілість політичних партій, проведення глобальних політичних дискусій, а не імітації їх зі спрямуванням лише на виборчі перегони, – це поштовх до розвитку суспільства.

Це сприятлива основа для економічних реформ, зміцнення банківської та фінансової систем. На моє глибоке переконання, політична еліта має повернутися обличчям до цього.

Ось тоді ми зможемо легше здолати й зовнішні перепони, зовнішні ризики, які тягнуть нашу державу до нерозуміння у світі, до згортання відносин в економіці, політиці, соціальній сфері. Ось тоді нам під силу поліпшити імідж України на міжнародній арені» [159, с. 8].

Наведені варіанти класифікації банківських ризиків ми не вважаємо вичерпними. Але вони охоплюють найважливіші фінансові фактори і їх наслідки. Тому на практиці слід враховувати різні варіанти ризиків, зокрема: ретроспективні, поточні та перспективні; низькі, помірні та повні; політичні та економічні; зовнішні та внутрішні, а також – виробничі, комерційні, фінансові; допустимі, критичні, катастрофічні ризики. Важливо їх своєчасно спрогнозувати і надійно управляти ними, уникаючи важких наслідків, не лише ризиків, але й найбільш поширених незаконних операцій, що провадяться через банківську систему, про що йтиметься у наступному підрозділі.

3.2. Характеристика найбільш поширених і небезпечних незаконних операцій в банківській системі та боротьба з ними

В умовах розвитку посттоталітарного суспільства стрімкого поширення набуває тіньова економіка як наслідок криміналізації економічних процесів. У зв'язку з цим введено термін кримінальної безпеки, яка представляє собою такий «різновид безпеки, який не має конкретного носія, але сильно впливає на економічне положення держави (економічні злочини, криміналізація суспільства тощо) та її мешканців (вбивства, грабежі, насильство, крадіжки тощо). Одним із характерних проявів криміналізації посттоталітарного суспільства є зростання частки тіньової економіки в сукупності економічної діяльності, зростання злочинності.

Динаміка зростання основних показників економічної злочинності у 1998-2000 рр. теж збереглася.

Обсяги показників «тіньової» економіки, за різними оцінками, становлять від 40 до 75 відсотків валового внутрішнього продукту (ВВП). Так, наприклад із 30 млн тонн нафти, завезеної в Україну у 1992 році, 8 млн тонн було переправлено контрабандою за кордон і перепродано. Із 5 млрд доларів, які того ж року Україна заробила за рахунок експорту нафтової продукції, державна казна отримала лише 97 млн доларів [81, с. 53].

«Тіньова» економіка сьогодні реально загрожує не лише економічній безпеці, але і її складовим (фінансовій, зовнішньоекономічній тощо).

«Серед основних форм тіньової економіки у сучасній економічній літературі виділяють, як правило, такі:

– неофіційна економіка – легальні види економічної діяльності, в межах яких має місце виробництво товарів і послуг, що не фіксуються офіційною статистикою, укриття цієї діяльності від податків;

– фіктивна економіка – економіка приписів, спекулятивних операцій і всілякого роду шахрайства, пов'язаних з одержанням і передачею грошей;

– підпільна економіка – всі заборонені види економічної діяльності.

До підпільної економіки, що безпосередньо підлягає кримінальному світові, належать: торгівля зброєю, наркотиками, гральний бізнес, проституція тощо» [81, с. 54].

Побили усі рекорди корупція керівництва, криміналізація економіки країн пострадянського простору. Україну роз'їдає всепроникліва і глибока корупція, організована злочинність. На думку Президента Леоніда Кучми, в Україні ще в 1994 р. сформувалась «п'ята влада» – влада мафії, що стрімко підминає під себе всі інші гілки влади – законодавчу, виконавчу, судову, засоби масової інформації. Тільки в кінці 1999 р. Президент задекларував рішучу боротьбу з мафією, корупцією та організованою злочинністю [83, с. 133].

Аналіз матеріалів багаторічної практики свідчить, що незаконні операції в БСУ умовно поділяються на дві частини: ті, які застосовуються безпосередньо у банківських установах; ті, якими користуються підприємницькі структури з використанням банківських установ. Виходячи з цього ми вивели загальну структуру і класифікацію складових елементів незаконних операцій, яка схематично зображена на таблиці 5.

Розглянемо ці складові розкрадання кредитів та механізм їх здійснення. Зокрема, розкрадання кредитів, які надаються невеликим комерційним структурам (найчастіше таким, що утворились тільки спеціально з метою отримання такого кредиту), або приватним особам. Наприклад, після одержання позичених коштів, їх перетворення на готівку або іншої матеріалізації (через конвертацію в ВКВ або придбання товарів) боржник зникає. На перший погляд, це діяння виглядає як шахрайство з боку одержувача кредиту. Так воно частіше за все й буває, і тут не має значення, що він є посадовою особою у себе на підприємстві. Такі дії треба кваліфікувати: для приватних осіб — за ст.83 КК України як «Розкрадання державного або колективного майна шляхом шахрайства» – оскільки відносно коштів банку, одержаних у кредит, вони не є посадовими особами; для посадових осіб – за ст.191 КК України «Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем», та ст. 222 КК України «Про шахрайство з фінансовими ресурсами». Нерідко ініціаторами або співучасниками таких дій є відповідні посадові особи банків, які мають від цього «бізнесу» певний «відсоток» (як правило, 10– 50% від

кредитованої суми). Для розкрадання кредитних ресурсів часто створюються псевдопідприємства. Розкрадачі з числа банківських працівників надають їм допомогу в одержанні кредитів та перетворенні їх у готівку. Після розподілу одержаних коштів, при першій появі з перевіркою співробітників правоохоронних органів, «боржник» «кидає» своє підприємство і зникає. У таких випадках посадові особи банків є організаторами розкрадання довірених їм коштів. Їхні дії слід кваліфікувати як розкрадання, а діяння боржника – як співучасть у розкраданні.

Співробітники правоохоронних та інших контролюючих органів, які проводять перевірку, повинні знати, що зацікавлений банківський працівник намагається, наскільки це можливо, переносити (часто неодноразово) строк повернення такого кредиту щонайменше до офіційної перевірки. Перенесення строку може відбуватися шляхом протекції такому «боржнику» і укладання з ним відповідних додаткових угод щодо пролонгації строків повернення кредиту або простим виправленням контрольних строків в облікових документах (цей спосіб характерний для великих комерційних акціонерних банків). Однак найбільш небезпечні злочинці, привласнивши одержані у кредит кошти, не приховуються, а поки можна, переносять строк повернення кредиту шляхом службового підлогу та підробки документів про дебіторську заборгованість, тобто про тимчасову відсутність у них коштів через затримку їм платежів, за нібито відправлену ними продукцію, надані послуги чи виконані роботи. Якщо строк повернення кредиту відкладати вже неможливо, то імітується реорганізація, самоліквідація, чи ініціативне банкрутство юридичних осіб. Порядок і умови визначення юридичних осіб банкрутами визначені в Законі України «Про відновлення платоспроможності боржника або визнання його банкрутом». Мета закону – задовольнити претензії кредиторів, але борги не завжди можуть бути забезпечені банкрутом.

При вивченні підстав банкрутства слід звернути увагу на те, чи не є воно навмисним або псевдобанкрутством, коли боржник заявляє про свою неплатоспроможність, а сам приховує чи передає за допомогою псевдоугоди, чи інакше майно у володіння інших осіб. Всі такі факти та випадки фіктивної застави за підробленими або юридично неправомірними документами, або застави без її реального майнового забезпечення, – є доказами шахрайства з боку боржника. У документуванні розглянутого шахрайства є певні труднощі, які полягають у тому, що одержання кредиту та його повернення відноситься до сфери фінансових та цивільно-правових стосунків, юридичний та економічний аналіз яких є дуже складним і не завжди призводить до реальної можливості притягнення боржника до кримінальної відповідальності.

Поряд з цим, у разі одержання та відпрацювання інформації про шахрайство з кредитними ресурсами відповідні працівники правоохоронних органів для збирання доказів наміру на неповернення кредиту повинні вживати всі надані їм законом процесуальні засоби. Необхідно пам'ятати, що злочинні зв'язки і наміри учасників розкрадання слід документувати на стадії перевірки. Серед різних правопорушень перш за все потрібно встановити докази щодо наміру, спрямованого на розкрадання грошових коштів, наданих в кредит. Це можна зробити тільки простеживши у комплексі весь технологічний ланцюжок протиправних дій учасників угоди, починаючи від працівників банку, підприємств-посередників (їх може бути ціла низка, як українських, так і зарубіжних) до вкладення на розрахункові рахунки розкрадачів або іншого використання частки розкрадених коштів, тобто потрібна глибока перевірка на всіх етапах кредитних банківських операцій.

Розкрадання грошових коштів нерідко провадиться під виглядом їх конвертації у ВКВ, у тому числі з приховуванням валюти за кордоном, що «продовжує залишатися одним із засобів незаконного збагачення ділків «тіньової» економіки»[114, с. 27]. Цей спосіб розкрадання грошових коштів у банках за механізмом схожий з попереднім способом, але тут гроші розкрадаються не шляхом видачі кредитів, а за допомогою перерахування великих сум підприємствам – посередникам під укладення угод на їх конвертацію у ВКВ. Каталізатором такого способу розкрадання стала та обставина, що у 1992 р. Україна вийшла з зони рубля. У банках накопичилася велика сума рубльової маси, яку до передачі в Росію слід було якимось чином випустити в обіг. Оскільки банки відповідно до ст.48 Закону України «Про банки і банківську діяльність» не мають права провадити торговельні операції, займатися виробничою діяльністю, то найбільш масштабним і легальним способом випуску в оборот грошових коштів є їх конвертація у валюту. За цих умов посадові особи комерційних банків знаходять (найчастіше за межами України) підприємства, які нібито можуть конвертувати гроші у ВКВ. Укладають з ними відповідний договір і перераховують визначену у договорі суму підприємству-посереднику, яке, за можливості, перетворює одержані кошти на готівку або матеріалізує через контракти на придбання товарів і ділить їх з ініціаторами перерахування грошей. Якщо сума велика і одержані кошти, зокрема і частку працівників банків, слід пустити в обіг, підприємство-посередник може передати їх як готівкою, так і безготівково, за фіктивними договорами, спільним підприємствам. Останні у договорах обумовлюють, що у випадку непоставки вказаних у договорі матеріальних цінностей, кошти буде повернуто вкладнику у ВКВ на еквівалентну суму по курсу аукціону на розрахунковий рахунок і в банк, які вкаже платник. Оскільки договір на

поставку матеріальних цінностей фіктивний від самого початку, то зарубіжне головне підприємство (співзасновник СП) за неврахованим листом підприємства-посередника чи банку-емітента цих коштів перераховує еквівалентну суму у валюті на відкриті за кордоном рахунки розкрадачів.

Поряд з цим, коли настає строк виконання умов за першим договором (на конвертацію грошових коштів), посадові особи банків, які надали ці кошти під псевдоугоду з метою маскування своїх злочинних дій, надсилають листа на адресу підприємства-посередника про розірвання договору і вимагають повернення перерахованої їм суми. Проте партнери за угодою гроші не повертають. Поки це можливо, триває листування, провадяться інші дії, що вуалюють розкрадання, а коли до перевірки підключаються правоохоронні органи, відповідальні за ці операції посадові особи підприємства-посередника зникають. Найчастіше вони виїжджають до країн далекого зарубіжжя, куди на їх рахунки головне підприємство – засновник СП – перерахувало частину валюти, одержаної за рахунок викрадених у банку грошових коштів. Як і в першому випадку, при розкраданні кредитів, так і в другому – при розкраданні грошових коштів, перерахованих на конвертацію у ВКВ, злочинний зв'язок і намір учасників розкрадання слід документувати на стадії перевірки. При цьому також необхідно мати на увазі, що серед маси розрізнених кримінально не караних правопорушень треба визначити і довести намір, спрямований на розкрадання випущених в оборот грошових коштів. Як і в попередньому випадку, це можна зробити лише простеживши у комплексі весь технологічний ланцюжок протиправних дій учасників угоди, починаючи від операцій працівників підприємств-посередників (їх теж може бути цілий каскад як українських, так і зарубіжних) до вкладення на розрахункові рахунки розкрадачами їх частки викрадених коштів, тобто потрібна оперативна перевірка на всіх етапах угоди.

Офіційним приводом на проведення всього комплексу слідчих дій зі збору доказів в обох останніх розглянутих способах злочинів можуть бути:

1. Винесення Господарським судом окремої ухвали про наявність у матеріалах справи обставин, які свідчать про склад злочину у діях однієї із сторін.

2. Наявність доказів, які свідчать про те, що службові особи фірми, які провадили конвертацію грошей, після прострочення строку виконання зобов'язань зникли і їх місцезнаходження невідомо, або встановлені інші обставини, що підтверджують їх можливі наміри привласнити одержані кошти шахрайським шляхом (псевдобанкрутство тощо).

При документуванні цих правопорушень велике значення має пошук підтвердження інформації про: використання отриманих грошей не за

призначенням; відсутність на розрахунковому рахунку вказаної комерційної організації грошових коштів; ліквідацію офісу або подання в договорі неіснуючої адреси; розпродаж майна цієї комерційної організації або незаконне оголошення її банкрутом; оформлення фіктивних застави, поруки або видача фіктивних векселів; подання підроблених банківських та інших документів для підтвердження «реальності» виконання угоди; конвертацію грошей комерційними організаціями, статутом яких непередбачена вказана діяльність. Для доказу злочинної діяльності розкрадачів можуть бути використані результати аналізу таких документів: договору, укладеного між учасниками угоди, на конвертацію грошей; витягу із розрахункового рахунку в банку про наявність і рух грошових коштів, які належать комерційній організації, що займається конвертацією; платіжного доручення на переказ грошових коштів організації, яка провадить конвертацію; документів, що знаходяться в банку при відкритті розрахункового рахунку; статуту комерційної організації; договору про оренду приміщень під офіс, або документи, що свідчать про фіктивність адреси підприємства; рішення Господарського суду про визнання вказаної комерційної організації банкрутом і матеріали, які свідчать про навмисне банкрутство; інших матеріалів, які можуть свідчити про шахрайські наміри учасників оборудки.

Коли інформація про такі правопорушення до співробітників контролюючих органів надійшла своєчасно, то документування слід вести на стадії договірного і наступних етапів кредитних банківських операцій. Разом з тим, встановити їх заздалегідь не завжди можливо. У таких випадках попередні етапи операцій з поля зору перевіряючих випадають. Тому для збору доказів потрібно якнайефективніше використовувати стадію реалізації матеріалів, коли між співучасниками злочину відбуватимуться координаційно-консультативні контакти, фіксація змісту останніх допоможе показати злочинний характер дій учасників псевдоугоди.

Розкрадання та привласнення грошових коштів відбувається також шляхом привласнення нарахованих відсотків за вкладами клієнтів або переказами коштів клієнтів (без їх відома) з депозитних рахунків на інші рахунки або у фонди. Привласнення службовими особами банку грошових коштів таким способом може відбуватися за рахунок: свідомо неправильного визначення відсотків по вкладах, частіше всього у випадках, коли на рахунку клієнта є не «кругла» сума, а також, коли грошові кошти лежать на рахунку у банку неповний календарний рік. Цьому сприяє як складність визначення відсотків, так і те, що не кожний громадянин може або знає, як перевірити правильність їх нарахування; щорічне нарахування відсотків на суму первісного вкладу, а не на суму фактичного залишку; переоформлення простого вкладу клієнта на терміновий вклад без його відома

з метою привласнення різниці в сумах нарахованих відсотків між терміновим і звичайним вкладом.

Збір доказів на стадії реалізації матеріалів полягає в пошуку, реєстрації, аналізі перш за все документів, які містять дані про звиконання тих чи інших операцій по вкладу. До таких документів належать: операційний щоденник; особистий рахунок; прибутковий ордер на прийняття готівки; прибутковий ордер (Ф. 63) (при безготівковому розрахунку), який складається на загальну суму платежів, що списані з рахунків вкладників за їх дорученням; книга реєстрацій ощадних книжок, які не затребувані клієнтами (Ф. 20); довідки про виведені залишки вкладів і суми нарахованих відсотків (Ф. 30); виписки (Ф. 19). Це дає можливість одержати інформацію про привласнення матеріально-відповідальними особами банку грошових коштів будь-яким способом, організувати проведення документальної ревізії за певний період, задокументувати дії працівників-правопорушників. Аналогічним способом можуть вчинюватися розкрадання грошових коштів шляхом нарахування дивідендів по акціях та інших цінних паперах, за якими передбачені виплати відсотків за користування банком вкладеними грошовими коштами, зокрема і грішми юридичних осіб.

У кожному випадку виявлення зловживань, вчинених працівниками банківських установ, повинно бути організовано суцільне звірення записів в ощадних книжках вкладників із записами в їх особистих рахунках і документами, які знаходяться в бухгалтерії банку. Для цього слід запросити клієнтів до філії чи відділення банку або здійснити таку перевірку за місцем проживання клієнтів. Крім того, доцільно перевірити об'єктивність записів в ощадних книжках працівників філії (відділення) банку, звертаючи увагу на суми безготівкових перерахувань. При встановленні останніх необхідно перевірити платіжні відомості на одержання заробітної плати та перекази Ф.1 і 10-а (за їх допомогою здійснюються безготівкові перекази).

Значного поширення останнім часом набуло також розкрадання облігацій державної позики та інших цінних паперів при купівлі їх від населення. Касири комерційних банків привласнюють частину цих облігацій та інших цінних паперів. Цей злочин передбачає й часткове неоприбуткування цінних паперів і невідображення касиром чи контролером в операційному щоденнику, а також у додатку до нього (контрольній відомості Ф. 56) суми їх вартості. Надалі неоприбутковані цінні папери продаються населенню, а гроші привласнюються. Скоєнню цього злочину притаманний попередній зговір між контролером, касиром і завідуючим філії чи відділення банку.

Окрему групу розкрадання грошових коштів вкладників складає повне або часткове їх неоприбуткування. Механізм цього злочину полягає у тому,

що контролер-касир комерційного банку під час приймання грошей від вкладників може частково або повністю не проводити їх по оперативному щоденнику і особистому рахунку вкладника, хоча в його ощадній книжці ці суми будуть відображені правильно. Розкрадання таким способом можливе, коли на цій операції працює один і той самий контролер-касир, адже його зміна призведе до викриття злочину. У практиці зустрічаються випадки, коли злочинці з метою уникнення викриття ведуть «подвійний облік», тому при документуванні розкрадань таким способом важливо своєчасно викрити і вилучити подвійну картотеку або інші документи «подвійного обліку». Подальша перевірка проводиться шляхом зустрічної звірки ощадної книжки вкладника, прибуткового ордера з операційним щоденником, реєстром та особистим рахунком клієнтів. Виявлені невідповідності у перших двох документах з іншими та почеркова експертиза стануть незаперечними доказами вчинення злочину.

Свої особливості мають незаконні операції, що вчинюються у підприємницьких структурах з використанням банківських установ. Протиправна діяльність у банківській системі в основному пов'язана із зловживаннями при оподаткуванні, при наданні кредитів, позичок: конвертацією, з подальшою крадіжкою грошових коштів через «ЛОРО-рахунки»; незаконною емісією цінних паперів банків, вексельним обігом, нецільовим використанням та розкраданням бюджетних коштів, приховування. Вивчення в Україні та інших країнах СНД досвіду боротьби із зловживаннями, які вчинюються посадовими особами підприємств (частіше комерційних структур) у співучасті з працівниками банківських установ, обгрунтований аналітичний прогноз можливих правопорушень дає підстави вважати, що зараз, за умов первинного накопичення капіталу, ця категорія зловживань найбільш поширена та суспільно небезпечна і, як уже згадувалося, здатна підірвати основи економіки і остаточно зруйнувати фінансову систему країни.

За способом ці операції часто вчинюються шляхом розкрадання матеріальних, грошових коштів чи вільноконвертованої валюти і проводяться з використанням чекових книжок у комбінації з кредитовими та дебетовими авізо. Механізм розкрадання за допомогою чекової книжки у комбінації з кредитовим і дебітовим авізо розрахований на розкрадачів, які ставлять собі за мету «відмити» фіктивно утворені кошти і користуватися ними у легальному платіжному обігу. За технологією виконання суб'єктом цього злочину є посадові особи неплатоспроможних чи платоспроможних підприємств і обслуговуючих їх банків, які діють завжди у змові. З метою більш глибокого маскування процесу «відмивання» фіктивно утворених сум до злочину залучаються підприємства-одержувачі коштів за незабезпеченими чеками. Між підприємством-псевдоплатником і псевдо-

одержувачем складаються фіктивні угоди, за домогою яких провадиться серія перерахувань з метою завуалювати джерело та ініціатора фіктивно утворених коштів.

Один із видів розкрадання матеріальних або грошових коштів відбувається за допомогою незабезпечених чекових книжок. Перед тим, як перейти до висвітлення конкретного механізму вчинення зловживань шляхом використання чекових книжок, необхідно звернутися до особливостей діючого порядку застосування чеків у платіжному обігу, тоді ми зможемо зрозуміти не тільки ті способи зловживань, які ми розглянемо, а й інші варіанти корисливих посягань, що можуть вчинятися за допомогою використання чекових книжок. В основі механізму їх вчинення лежить утворення фіктивних грошових коштів та їх випуск у безготівковий платіжний обіг. Засобом «відмивання» таких коштів є використання незабезпечених чекових книжок при взаєморозрахунках суб'єктів фінансово-господарської діяльності, тобто підприємств, організацій та установ, в тому числі банківських та інших кредитно-фінансових закладів.

Як зазначалося раніше, оформлення незабезпечених чекових книжок може провадитись від імені псевдопідприємств як неплатоспроможних так і платоспроможних. Тут, як і при використанні фіктивного авізо, від статусу суб'єкта злочину чи варіанта його виконання залежить відповідна кваліфікація дій правопорушників. У деяких випадках ці зловживання кваліфікуються як підробка документів, шахрайство або розкрадання в особливо великих розмірах шляхом шахрайства, а в інших – ці самі дії з огляду на певні обставини є лише порушенням банківського та цивільного законодавства.

Практика розслідування правоохоронними органами кримінальних справ показує, що цей спосіб зловживання поділяється залежно від варіанта використання незабезпеченого чека. Перший варіант – коли фіктивно утворені грошові кошти за допомогою незабезпеченого чека та супутніх йому угод, доручення на право отримання цінностей у розмірі суми чека використовуються у прямому розрахунку з потерпілим підприємством. Другий варіант, коли з метою більш глибокого маскування фіктивно утворених коштів чек і супутні йому псевдоугоди використовуються у комбінації з кредитовим і дебітовим авізо та залученням до зловживання співучасників ще одного або кількох підприємств. При 1-му варіанті незабезпечений чек може бути оформлений від імені будь-якої категорії зазначених вище підприємств, тобто від прсевдопідприємства як неплатоспроможного, так і платоспроможного. Однак у всіх випадках чек і супутні йому документи використовує приватна особа – шахрай. Роздобути ці документи з відповідними печатками він міг шляхом копіювання, підробки або одержати за хабарі та іншим способом у посадових осіб підприємств та

комерційних банків. Заволодівши такими документами, шахрай прибуває на підприємство-постачальник, домовляється про закупку певної кількості товару, розплачується чеком, і негайно вивозить його своїм транспортом. На цьому механізм розглянутого варіанта розкрадання цінностей, практично, закінчується. Дії зловмисника кваліфікуються як підробка та використання підроблених документів за ст. 358 КК України або за ст.190 – Шахрайство. Дії службових осіб, які давали шахраю бланки з відбитками печаток за винагороду, кваліфікуються як одержання хабара і співучасть у підробці документів. Разом з тим, такі службові особи можуть бути організаторами шахрайства, тобто розробляють технологію розкрадання, підбирають його виконавця та ділять з ним викрадене майно. Тому при розшуку шахрая з викраденим майном, особливо, коли розшук ведеться по гарячих слідах, треба тримати постійно в полі зору службових осіб підприємницьких структур і банку-чекодавця, чиї печатки є на чекових книжках, угоді та дорученні.

Порядок подальшого проходження чека, одержаного продавцем продукції, визначений у Положенні Національного банку «Про безготівкові розрахунки в господарському обороті України». Підприємство-чекодавець здає отриманий за товар чек в обслуговуючий його банк, де складають реєстр, погашають чек штампом банку, виписують дебітове авізо і відправляють всі ці документи з одним примірником реєстру у банк чекодавця для підтвердження чека. Тут і з'ясовується, що чек фіктивний. Слід відзначити деякі особливості в технології зарахування коштів за отриманими чеками. Якщо між банком чекодавця (покупця) і банком чекодержателя (продавця товару) є кореспондентські зв'язки (тобто відкриті коррахунки), то сума на рахунок чекодержателя банком буде зарахована відразу після подання чека.

Коли кореспондентських зв'язків між цими банками немає, то кошти на рахунок чекодержателя зараховуються тільки після отримання підтвердження суми з банку чекодавця. До тих пір ці кошти враховуються на забалансовому рахунку 9930 «реєстри чеків, що чекають оплати» у банку чекодержателя. Щодо першого способу розкрадання, то різниці немає, чи зараховані кошти на рахунок чекодержателя, чи віднесені на позабалансовий рахунок. Коли прийде відповідь з банку чекодавця, що чек підроблений, зараховані кошти з рахунку чекодержателя будуть зняті як фіктивно утворені, а товар чекодавцем вже вивезено.

Першою ознакою незабезпеченості чека є те, що покупець згоден придбати товар за значно вищими цінами, ніж вони склалися на ринку. Таким чином шахрай-покупець зацікавлює продавця відпустити товар, не чекаючи підтвердження забезпеченості чека, тим більше, що оплата чеком відповідає умовам попередньої оплати, яка запроваджена в останні роки.

Раніше було навпаки, пріоритет надавався попередньому відвантаженню товарів. Однак це було в межах єдиної системи держбанку та за інших економічних умов, коли в платіжний обіг фактично було неможливо випустити фіктивно утворені кошти. Цей стереотип дорого обійшовся багатьом підприємствам. В умовах масових неплатежів за відпущені товари, поширення практики безтоварних псевдоугод між комерційними структурами країн СНД за незабезпеченими чеками та фіктивними кредитовими авізо на рахунках багатьох підприємств України, інших країн СНД знаходилися мільярди таких фіктивно утворених сум. Це значно вплинуло на інфляційні процеси, а з іншого боку, коли такі факти виявились, з рахунків потерпілих кошти вилучалися, що завдало їм великих збитків.

До впровадження обмежень щодо розрахунків чековими книжками тільки в межах України незабезпечені чеки найчастіше використовувалися шахраями країн СНД. Наприкінці 1992 р., в зв'язку із зловживаннями за допомогою незабезпечених чекових книжок, НБУ ввів порядок, який передбачає платіжний обіг чеків тільки в межах країни чекодавця, але це не виключає таких зловживань при розрахунках чеками між підприємствами, розташованими на території України. У першому кварталі 1993 р. чеком можна було розраховуватись тільки у межах області, але це також не виключало зловживань при їх використанні для розрахунків із суб'єктами, що знаходились у регіонах, де проходять міжнаціональні та інші воєнні конфлікти. Злочинці розуміють, що перевірити забезпеченість такого чека практично неможливо. Поряд з тим, суверенізація та комерціоналізація банківських систем підштовхнула до розпаду комплексної системи міжбанківських взаємозвірок як між установами банків країн СНД, так і між комерційними банками в межах кожної новоствореної країни окремо. За таких умов випуск у безготівковий платіжний обіг фіктивно утворених грошових коштів досяг значних розмірів. У зв'язку з цим за домовленістю урядів країн СНД в розрахунки суб'єктів господарювання введена попередня оплата, але всупереч логіці, це не зняло проблему неплатежів. Кілька разів проводився їх взаємозалік у зв'язку із виходом України з рубльової зони. У квітні 1993 р. заборгованість України Росії складала 300 млрд, а у грудні 1993 – 5,1 трлн карбованців.

Найбільш ефективним захистом підприємств і банків від збитків при розглянутому варіанті розкрадання є затримка відвантаження товарів чекодавцю до надходження підтвердження про забезпеченість коштами пред'явленого ним чека. Однак у другому варіанті розкрадання, тобто за допомогою використання чекової книжки у комбінації з кредитовими та дебетовими авізо, простим запитом у банк чекодавця захиститись неможливо, тому що у цьому випадку працівники банку-платника брали

участь у створенні фіктивних коштів, і на запит банку-чекоутримувача вони дадуть позитивну відповідь.

Свої особливості має розкрадання коштів посадовими особами неплатоспроможних чи платоспроможних підприємств з використанням платіжних доручень та фальшивих кредитових авізо. Механізм утворення фіктивних грошових коштів, спосіб їх «відмивання» та вилучення за допомогою фальсифікованих кредитових авізо посадовими особами неплатоспроможних підприємств в цілому схожий з попереднім, але має деякі особливості.

Неплатоспроможні підприємці, як і псевдопідприємці, використовують ті самі форми документів: угоди, незабезпечені платіжні доручення підприємства, фіктивне кредитове авізо. Поряд з цим, на першому етапі зловживання дії посадової особи підприємства відрізняються від дій псевдопідприємця. Останній підробляє платіжні документи і подає їх від імені своєї чи іншої псевдоорганізації до чужого банку, де він не має рахунку і не є клієнтом. Тому дії втягнутих у процес «відмивання» фіктивних грошових коштів банківських працівників виглядають так, ніби шахрайство вчинене без їх відома. Хоча цей обман, як уже зазначалося вище, перевірити неважко. Більше того, у попередньому прикладі з'ясовано, що банківські працівники у разі сумніву у достовірності пред'явлених документів повинні направити запит у РКЦ з приводу їх достовірності.

Щодо посадових осіб неплатоспроможних підприємств, то вони звертаються з незабезпеченим платіжним дорученням безпосередньо у банк, що обслуговує їх підприємство, де його рахунок, на якому чітко відображено, є там кошти чи немає. Тому утворення фіктивних грошових коштів, їх «відмивання» проходить тільки у змові з працівниками банку. Останні бачать, що на рахунку підприємства немає відповідних коштів. Більш того, у Правилах бухгалтерського обліку чітко обумовлено режим робочого дня обліково-операційних працівників, графік проходження документів по всіх ділянках їх опрацювання, порядок перевірки записів в особистих рахунках, інших облікових документах, а також визначено конкретних операційних працівників, які виконують конкретні обов'язки на дорученій їм ділянці роботи. У відділеннях банківських установ, де в обліково-операційному апараті нараховуються до п'яти осіб, документообіг і внутрішньобанківський контроль організовано таким чином: один відповідальний працівник веде розрахункові, позичкові, поточні та інші рахунки всіх підприємств, організацій, колгоспів; рахунки прибутків, бюджетні поточні рахунки, рахунки страхових організацій та капітальних вкладень веде другий відповідальний працівник; рахунки внутрішньобанківського значення, картотеки МФО (міжбанківських обігів), друкування авізо по МФО, опрацювання вхідної та відправка вихідної

пошти й телеграфної кореспонденції доручено третьому відповідальному працівнику. В останньому випадку обов'язки може бути поділено між двома відповідальними працівниками, або вони повністю чи частково виконуються заступником головного бухгалтера під контролем головного бухгалтера. Формування меморіальних ордерів дня виконує заступник головного бухгалтера. Він же складає (або веде) бухгалтерський журнал шляхом реєстрації документів дня, з доповненням касових оборотів за день і складає щоденний баланс. (У банківських установах, де обсяг операцій невеликий, журнал реєстрації операцій за день може вестися шляхом підрахунку документів з підведенням підсумків по дебетовому обігу балансових рахунків, але ці документи мають бути зброшуровані, щоб їх не зарахували вдруге).

Головний бухгалтер перевіряє щоденний баланс, виконує всі контрольні функції по касових операціях, а також звіряє аналітичний облік із синтетичним. У великих підрозділах обліково-операційних апаратів ці види робіт виконують групи або відділи працівників, а контрольні функції виконують керівники відділів чи інші провідні фахівці. Хто конкретно займався обслуговуванням того чи іншого неплатоспроможного підприємства, можна з'ясувати у відповідних операційних працівників. Встановити це можна за їх підписами на документах. Однак практика показує, що до таких псевдоопераций, як правило, відношення мають не тільки прямі виконавці цих операцій, а й працівники (головний бухгалтер та голова правління) комерційного банку. Крім того, щоб не вдаватися до складних дій з метою приховування у балансі фіктивно утворених сум, ці операції не відображаються у документах аналітичного та синтетичного обліку. Тобто не робляться відмітки про операції в особистих рахунках юридичних осіб, не вносяться дані у бухгалтерський журнал реєстрації операцій дня, зведені карточки і щоденні перевірочні відомості, фіктивно утворена сума не відображається у щоденному балансі.

Неплатоспроможні підприємці-шахраї та їх співучасники-банківські працівники на шляху відмивання фіктивно утворених коштів та їх матеріалізації у товар, готівку чи вільноконвертовану валюту іноді вступають у змову почергово з кількома підприємствами (на території України), роблять два-три цикли перекладок фіктивно утворених сум перед тим як їх матеріалізувати у цінності. Мета цих дій одна – завуалювати джерело й ініціаторів фіктивно утворених коштів та ускладнити перевірку і збір доказів про злочинну діяльність зловмисників. В умовах інтернаціоналізації злочинності та процесуальних бар'єрів, які виникли з розпадом єдиного правового поля між країнами колишнього СРСР, це досить ефективно слугує злочинцям. Платіжне доручення неплатоспроможного підприємства банк забезпечує всіма наявними у нього

кредитними ресурсами. Однак без відповідного оформлення кредиту, банківських проваджень за рахунком клієнта та іншими обліковими документами, сам факт наявності вільних кредитних ресурсів у банку ще не означає, що така операція ними забезпечена. Неплатоспроможному підприємству може бути надана позичка до випуску в обіг цього платіжного доручення, зарахована на його рахунок, потім для оплати товарів за угодою знята з рахунку та проведена за наведених вище документами синтетичного обліку банку (по бухгалтерському журналу реєстрації банківських операцій, зведених картках балансу тощо), і переказана в РКЦ для перерахування фірмі. У такому разі була б переведена реальна сума, що у свою чергу спричинило б зменшення кредитних ресурсів банку. Відправлена у РКЦ фіктивно утворена сума не зменшила кредитні ресурси банку, а стала засобом вчинення шахрайства відносно цінностей фірми, оскільки за відпущений реальний товар остання одержала фіктивні грошові кошти, які після викриття злочину були зняті з її рахунку.

Аналогічним способом вчинюються злочини, якщо фіктивне платіжне доручення, а за ним і фіктивне авізо оформляються від імені неплатоспроможної організації. Хоча на рахунку підприємства-платника кошти є, але у змові з банківськими працівниками з його рахунку під суму, вказану у загальних фіктивних платіжних документах, грошові кошти не знімаються. Для розрахунку під ту чи іншу угоду шляхом службового підлогу направляється фіктивно утворена сума. Як і в попередньому випадку, операція не реєструється у документах дня аналітичного і синтетичного обліку. При викритті таких злочинів шахраї, як правило, висувають алібі, що вони мали сумнів відносно своїх партнерів щодо поставки останніми цінностей, обумовлених в угоді, але мали намір розрахуватися реальними коштами після того, як товари постачальником будуть їм відвантажені або доставлені.

Попередження такого зловживання на початковій стадії викликає ускладнення при доказуванні суб'єктивного боку складу злочину, тобто злочинного наміру шахраїв. Тому правильний вибір моменту легалізації матеріалів перевірки має важливе значення. Крім того, шахраї, як правило, одержані за угодою від партнерів товари на своєму підприємстві не приховують. Це пояснюється тим, що з рахунку їх підприємства грошові кошти не знімались і при зарахуванні товару у балансі фінансово-господарської діяльності виникнуть надлишки. Тому отриманий за фіктивні грошові кошти товар реалізується без оприходування, оптом або у роздрібній торгівлі як за готівку, так і за безготівковими розрахунками. У разі безготівкових розрахунків на суму реалізованого товару між продавцем і покупцем може складатися псевдоугода на начебто виконані роботи чи надані послуги. Продаж товару за безготівку викликаний тим, що не

кожний покупець товару може роздобути потрібну суму готівки, а з іншого боку, при безготівкових розрахунках підприємці-розкрадачі товар можуть продати дорожче.

Заслуговують на окрему увагу зловживання за допомогою платіжного доручення у супроводі фіктивного кредитового авізо. В основі цього виду зловживань є незабезпечене коштами платіжне доручення підприємства та фіктивне кредитове авізо банку. Відповідна кваліфікація дій правопорушників залежить від суб'єкта чи варіанта використання цих платіжних документів. У деяких випадках ці зловживання кваліфікуються як: підробка документів; шахрайство або розкрадання в особливо великих розмірах шляхом шахрайства, а в інших – ці самі дії за певних обставин кваліфікувати як злочин неможливо.

Розглянемо ці випадки залежно від суб'єкта вчинення зловживань. Вище ми відзначили, що фіктивне авізо може бути використане: шахраєм-організатором псевдопідприємства чи підроблювачем платіжних документів; посадовими особами неплатоспроможних чи платоспроможних підприємств. Дії організатора псевдопідприємства, підроблювача платіжних документів, на першому етапі вчинення злочину відрізняються від дій посадових осіб інших зазначених підприємств і відповідно до їх статусу, кваліфікуються інакше за нормами КК України. Псевдопідприємець має роздобути та підробити бланки платіжного доручення підприємства (частіше для ускладнення перевірки від імені іншого псевдопідприємства країн СНД), кредитового авізо з відбитком печаток комерційного банку або розрахунково-касового центру держбанку (з кінця 1991 р. – до початку 1993 р. перекази з країн та до країн СНД проходили обов'язково через РКЦ держбанків цих країн. Таким чином контролювалося товарне покриття та взаєморозрахунки за зустрічними угодами. Зараз ці функції виконує центр міжнародних розрахунків). Якщо підроблювач документів дав службовій особі відповідної установи за бланки чи відбиток на них печатки винагороду, то в його діях також присутній склад злочину, передбачений ст.369 КК України (давання хабара), а у діях службової особи, яка отримала хабара – склад злочину, передбачений ст. 368 КК України, та співучасть у підробці документів (статті 26, 27, 358 КК України).

На цьому перший етап підготовки до основного злочину – розкрадання грошових коштів чи матеріальних цінностей, псевдопідприємець закінчив. Така деталізація дій співучасників потрібна, бо: статус службових осіб неплатоспроможних підприємств та псевдопідприємця різняться між собою й інакше кваліфікується згідно із КК України; цей спосіб розкрадання показує, що у зв'язку з широкою географією злочину та процесуальними бар'єрами, які виникли після розпаду єдиного правового

поля (СРСР), зібрати повністю матеріали щодо всієї схеми злочину і його співучасників не так просто.

Тому, якщо на кожному етапі у частини співучасників самостійний склад злочину, то з'являється можливість порушити проти них кримінальну справу, а це дає підставу проводити певні процесуальні дії на території країн СНД до збирання доказів і розслідування злочину у повному обсязі, або притягнути до відповідальності підроблювача документів, зокрема і за підготовку (замах) до шахрайства (статті 14 і 190 КК України). Крім цього, своєчасна ізоляція підроблювача документів на початковому етапі злочину може стати важелем для здобуття доказів щодо хабарників, які поставили потрібні печатки на авізо, інші платіжні та супутні їм документи (доручення, угоди, платіжні доручення від третіх організацій тощо). Щодо посадових осіб неплатоспроможних підприємств, то відносно них на першому етапі підготовки до основного злочину таких важелів немає. Дії останніх на цьому етапі підготовки до розкрадання мають ознаки службового підлогу та зловживання службовим становищем (статті 366, 364 КК України), але під кваліфікуючі ознаки цих злочинів вони не підпадають. Це ускладнює подальше збирання доказів. Варіанти вчинення таких злочинів можуть бути різними: псевдопідприємці розширюють географію походження фіктивних документів до меж країн СНД; псевдопідприємці звужують географію проходження фіктивних платіжних документів у межах України; з метою ускладнення їх викриття за допомогою псевдоугод роблять кілька перекидок платіжних документів через відповідні банківські установи від одного до другого підприємства на території України або інших країн СНД, доки не знайдуть найпридатніший спосіб вилучення готівки, товарів чи вільноконвертованої валюти.

До цієї групи способів проведення незаконних операцій у КБС відноситься також розкрадання коштів чи ВКВ з використанням чекових книжок у комбінації з кредитовим та дебітовим авізо; створення фіктивних підприємств.

Різке зростання злочинності в економічній сфері викликає справедливе занепокоєння, а також необхідність вжиття заходів і перш за все правового регулювання кредитно-фінансової сфери та підвищення відповідальності за правопорушення в цій сфері.

Оскільки «відмивання» коштів є одним із найскладніших і найпоширеніших злочинів, розглянемо його особливості в БСУ окремо.

Як повідомляє «Ділова столиця» у департаменті держслужби з боротьби з економічною злочинністю МВС скаржаться на те, що банки не надають необхідну інформацію. А в подібні підрозділи Служби безпеки України інформація поступає. Співробітництво з фінансовими установами визначає й низку злочинів, що виявляються. Якщо в МВС «ДС» повідомили, що

більшість зловживань виявлена при операціях з металобрухтом, то в СБУ акцентують увагу на фінансових операціях. «Останнім часом зловмисники активно використовують кримінальні схеми, завдяки яким здійснюються зовні легальні операції по обналічуванню засобів, у тому числі і з наступною конвертацією їх в іноземну валюту. Найбільше поширення ці факти отримали при здійсненні зовнішньоекономічної діяльності. Актуальним залишається використання офшорних компаній для відмивання брудних грошей, більшість злочинних механізмів у фінансовій сфері пов'язано зі створенням і використанням фіктивних підприємств», – повідомив «ДС» начальник прес-центру СБУ О. Скрипник. Він також підкреслив, що велика частина відомостей про такі правопорушення була отримана на підставі запитів у банківські установи.

Серед найбільш резонансних останнім часом фігурує справа, відкрита дніпропетровським підрозділом СБУ з боротьби з організованою злочинністю. За інформацією служби, в одному з місцевих банків протягом тривалого часу проводилися фінансові операції по легалізації засобів, прихованих від оподатковування. У ході розслідування справ, відкритих за цими фактами, фігурує сума в 500 млн грн, що вдалося легалізувати через банківські установи. Меншим виявився розмах харківських угруповань – там через спеціально відкриті 24 фіктивні фірми було переведено за кордон більше 30 млн грн. У розкраданні 7 млн грн обвинувачені й арештовані в Черкаській області дев'ять організаторів і активних учасників злочинного угруповання (була доведена їхня причетність до крадіжки бюджетних коштів). У цьому випадку, за словами співробітників СБУ, першу скрипку також грали місцеві співробітники банків. Усього обвинувачення було висунуто 20 особам («ДС» № 14 від 8.04.2002 р.). Ця проблема заслуговує самостійного розгляду, що буде висвітлено у наступному підрозділі.

3.3. «Відмивання» коштів через банківську систему та його виявлення

«Відмивання» грошей досить поширене у світі явище, наприклад, у США через банки було «відмито» близько трильйона «брудних« грошей [161], за оцінкою представників уряду США у світі «відмивається» близько трьох трильйонів доларів, не повертаються в Україну навіть ті кошти, які переведені за кордон, зокрема у США, і злочинне походження яких не викликає сумніву (справа П.Лазаренка).

Проаналізувавши платіжний баланс, фахівці банку з'ясували, що з України шляхом продажу через офшорні зони акцій за останні роки спритні ділки «відмили» мільярди доларів. Зокрема, у 2000 р. – 385 млн, у 2001 р. –

898 млн, у 2002 р. – 2,271 млрд дол США. Національний банк розробив і зареєстрував у Міністерстві юстиції України відповідний наказ, яким передбачається запровадження ліцензування операцій з купівлі-продажу акцій за межами держави. Цей крок не перешкодить діяльності чесних торговців цінними паперами і продемонструє серйозність намірів України щодо боротьби з «відмиванням брудних» грошей.

«Відмиванням» грошей називається процес, шляхом якого приховується справжнє походження та, в деяких випадках, справжній власник грошей чи іншого майна. При складній організації системи «відмивання» грошей, вона включає також і прикриття для джерела їх походження. Для багатьох різновидів діяльності, як відверто кримінальної, так і просто суспільно не прийнятої, «відмивання» грошей є життєво необхідним процесом. «Відмиваються» гроші, отримані від наркобізнесу, інших форм організованої злочинної діяльності, з метою ухилення від сплати податків, прикриття корупції офіційних осіб. Зростаюча інтегрованість світової фінансової системи, ліквідація бар'єрів для переміщення капіталу сприяє спрощенню процесу «відмивання» і, відповідно, ускладнює процес його моніторингу.

Процес відмивання грошей з певною мірою умовності може бути поділено на три фази (стадії).

Розміщення – гроші, переважно у формі готівки, вводяться до фінансової системи. Ця фаза є найнебезпечнішою з погляду можливості виявлення правоохоронними та іншими контролюючими органами. Готівкові гроші розміщуються у банках, обмінних пунктах, страхових компаніях, брокерських конторах, шляхом поштових переказів тощо або через розміщення готівки у закладах, що інтенсивно працюють з готівкою, – ресторанах, казино, магазинах, у першу чергу, таких, що торгують коштовними речами. Використовуються імпортно-експортні компанії, фірми з торгівлі нерухомістю. Казино переводять гроші у фішки, потім у зворотному порядку – фішки у готівку чи чеки. Саме на цій фазі найефективнішою є протидія «відмиванню» грошей, причому на перше місце тут виходять не правоохоронні заходи, а застосування ефективних регуляційних правил для фінансової системи.

Розшарування (або ешелонування) – стадія, на якій гроші відмежовуються від джерела свого походження шляхом створення складних «шарів» фінансових трансакцій, зокрема, із застосуванням банківських рахунків на підставних осіб. Метою є ускладнення моніторингу їх переміщення та надання анонімності. Цей процес також включає зміщування «законних» та «незаконних» прибутків, використання накладних та акредитивів на неіснуючі поставки, перекази на підставні фірми.

Інтеграція – фаза, на якій грошам надається видимість отриманих законним шляхом. Незаконні надходження повертаються в економіку шляхом банківських позик, що не викликає потреби у сплаті податків, через придбання коштовних речей, нерухомості, акцій та облігацій.

Таку власність може бути конфісковано через кримінальний процес лише у тому разі, коли її можна безпосередньо «прив'язати» до джерела надходження. Цьому, зазвичай, перешкоджає вся система відмивання грошей. Тому наявною тенденцією у сучасному світовому розвитку законодавства з питань відмивання грошей стало застосування в різних обсягах інструментів як для попередження «відмивання грошей», так і для припинення права власності на майно, отримане законним шляхом. Ця система ширше за все використовується в Сполучених Штатах, передбачається також новітнім законодавством Ірландії, що визнано найпрогресивнішим у цій сфері в Європейському Союзі, впроваджується зараз у Великій Британії. В тій чи іншій формі цивільно-правові механізми такого роду застосовуються і в деяких країнах континентальної системи права, таких, як Франція, Італія, Японія та Німеччина.

«Відмивання» грошей у країнах колишнього Радянського Союзу інколи плутають з досить відмінним процесом, що має іншу мету, але деякі спільні риси у реалізації, – мається на увазі виток капіталу. Насправді це зовсім різні процеси, які мають різні цілі, але механізми їх проведення спільні у тому, що обидва передбачають використання складних схем по переміщенню грошових коштів. У той же час, і більш-менш «класичне» «відмивання» грошей має місце – значні обсяги грошей, що приховуються від податків, потребують легалізації так само, як і гроші, отримані за фальшивим авізо, незаконними банківськими кредитами, іншим злочинним шляхом, якщо їх передбачається залучити до легальної економіки. Процес витоку капіталу сам по собі також передбачає його легалізацію, якщо гроші планується інвестувати в економіку країн, що мають жорсткі регуляційні правила та відповідне законодавство. Схеми з приховування джерела грошей використовуються і в тому разі, коли потрібно приховати не стільки джерело коштів, скільки їх власника.

Одним із методів розміщення грошей у фінансових інститутах є «смарфінг»[1]. Слід зазначити, що у значній частині країн (США, ЄС, Австралія, Японія, а також в Україні, ми говорили про це у § 1.2) регуляційними правилами для банків та інших фінансових установ передбачається обов'язкове повідомлення до центрального фінансового регулюючого органу щодо операцій з грошима на суму, що перевищує встановлений поріг, – в більшості випадків 10000 доларів США. При

[1] Від англійського "smurf" – гном, гремлін.

використанні «смарфінга» значні суми грошей розбиваються на менші за встановлений поріг і розміщуються у фінансових установах. Для цього використовується значна кількість осіб («смарфів»), які й проводять таке розміщення.

У деяких країнах світу, зокрема, Сполучених Штатах та Великій Британії умисне розбиття суми, що депонується, з метою ухилення від звітування до органів фінансового контролю, тягне за собою кримінальну відповідальність.

Після проведення такого депонування гроші переводять на один рахунок, після чого вони (у простих схемах) знімаються з рахунку у формі чека чи готівки або переводяться на інший рахунок.

Недоліками такого методу є потреба у значній кількості людей, що посилює можливість виявлення, повільність.

Інший спосіб розміщення передбачає використання «інсайдерів» – осіб, що використовують тим чи іншим шляхом своє корпоративне становище для власного збагачення. Взагалі, проблема «інсайдерів» виходить за рамки відмивання грошей і стосується широкого кола зловживань корпоративним службовим становищем та зловживань довірою. Так, особа, що завдяки своєму посадовому становищу у корпорації отримує інформацію, яку потім використовує на фондовій біржі для особистого збагачення, створює своїми діями загрозу для функціонування вільного ринку. Такі дії визнаються злочинними у багатьох юрисдикціях та тягнуть за собою відповідальність різного роду.

За відмивання грошей з використанням «інсайдера» співробітник фінансової інституції добровільно і свідомо надає сприяння у розміщенні великих сум готівки без доповідання до центрального контролюючого органу про підозрілу фінансову операцію.

Ще один спосіб, що використовуються при розміщенні готівки, – через «альтернативну» банківську систему. Ця система відома як «підпільні банки» (Азія), обмінні будинки (Латинська Америка) або системи «хавала» та «ханді» (Індія, Пакистан). Подібні системи роду існують протягом століть, замінюючи собою традиційні банківські, мають відділення в країнах Заходу, де переважно і отримуються гроші, що їх слід «відмити». Зокрема, найбільш інтенсивно вони застосовуються наркоділками із Центральної та Південно-Східної Азії («Золотий півмісяць» та «Золотий трикутник»).

У деяких країнах (наприклад, в Афганістані) нелегальна банківська система розвинута до рівня, що перевершує офіційну. Багато таких систем виникли в моноетнічних суспільствах через недовіру до офіційних інституцій, в інших випадках підпільні банки мають давню історію, а їх існування зумовлено цілою низкою соціальних та культурних факторів.

Важливість підпільних банків у процесі «відмивання» грошей починає все більше усвідомлюватися за останні роки. Широка міграція певних етнічних груп зробила цю систему інтернаціональною, що теж підвищило її роль у «відмиванні» з використанням існуючої банківської системи. Враховуючи негативний ефект, що його має підпільна банківська система на загальний обіг коштів у світі, вона не може ігноруватися тими, хто діє в межах звичайної банківської системи. На деякій стадії підпільна банківська система повинна переплітатися зі звичайною. Існує значна кількість різновидів такої системи – від складних структур, що контролюються китайськими етнічними угрупованнями, до відносно неформальних африканських структур, що займаються бартером та контрабандою грошей. Більшість систем не використовує переміщення готівки, а базується на певній системі символів. Китайські системи «Чіп» та «Чоп», індійська «Хавалах» діють в межах певних етнічних груп, інколи з урахуванням племених чи географічних додаткових ознак. Вони рідко передбачають фізичне переміщення готівки, обмежуючись системою символів, пов'язаних з структурою системи, які використовуються замість певної суми готівки. Система «Хавалах» є швидше засобом компенсації за рахунок пов'язаних трансакцій, але надаючи можливість накопичення та концентрації капіталу; реальні розрахунки між тими, хто фінансує систему, зведено до мінімуму. Ефективність банківської системи, яка практично не веде записів та іншої документації і при цьому має можливість для переказу значних сум грошей, є напрочуд привабливою для осіб, причетних до «відмивання» грошей. Їм часто доводиться створювати власні підпільні системи, і вони зацікавлені у використанні вже існуючих систем на комерційній основі. Закони та регуляційні правила, розроблені для боротьби з «відмиванням» грошей, не діють при використанні підпільних банків.

Контрабанда готівки, як і раніше, залишається поширеним інструментом при розміщенні грошей. Незважаючи на ризик, привабливою стороною цього методу є те, що в разі успішної реалізації, дозволяє повністю ліквідувати видимий зв'язок між грошима та їх походженням.

Електронні перекази грошей провадяться з різних місць, переважно в одній країні, на один банківський рахунок. Після накопичення на ньому відповідної суми, гроші переводяться до «фінансової гавані» – місця в країні із слабкими фінансово-регуляційними правилами.

Окрім наведених засобів можуть використовуватися і перекупка коштовних речей, експортно-імпортні операції тощо.

Змішування має місце у разі, якщо злочинна організація комбінує незаконно здобуті гроші із законними, а потім репрезентує всю суму як прибуток від законного бізнесу. Цей метод, за вдалого проведення, гарантує пояснення великим прибуткам, зокрема і отриманим готівкою як законно

отриманим. Якщо фінансова інституція не підпадає під підозру, наприклад, як така, що отримала занадто високий прибуток для своєї діяльності, змішування фондів практично неможливо ідентифікувати для правоохоронних органів.

Фірми прикриття – законно зареєстровані компанії, що займаються законним бізнесом, але, водночас, виступають як прикриття для незаконних операцій, у зазначеному випадку – для «відмивання» коштів. Така структура може проводити змішування незаконних коштів зі своїми законними прибутками. В цьому разі вона буде зменшувати витрати і збільшувати доходи.

Фіктивні компанії існують лише на папері, не займаються реальним бізнесом і виступають виключно як прикриття для незаконного переміщення коштів. Такі фірми надають прикриття корпоративної конфіденційності, приховують своїх реальних власників шляхом використання підставних осіб як власників, так і управляючих. *Підставні власники* – це особи, які заявляють про своє володіння майном, право власності на яке реально і в повному обсязі належить іншій особі. Фіктивні компанії можуть бути швидко утворені, набути статус юридичних осіб та в разі потреби, розпочати ділову діяльність, не заборонену законом.

Ознаками як фірм прикриття, так і фіктивних юридичних осіб є відсутність реклами, місцезнаходження у регіоні, де бізнес, що заявляється ними як основний, не може мати великих прибутків, належність обмеженому колу власників (на зразок ЗАТ), відсутність явної комерційної діяльності, перебільшена увага до забезпечення безпеки, використання контррозвідувальних заходів, а також наявність підставних осіб у штаті.

При розшаруванні грошей використовується незаконна банківська система. В цьому разі кримінальне угруповання набуває права власності над банком, потім засновує фіктивну фірму. Банк надає фірмі кредит, отримані гроші перераховуються на банківський рахунок, що належить угрупованню. Фіктивна фірма заявляє про неможливість повернення кредиту, отримує додатковий кредит для сплати відсотка за вже отриманий кредит.

Ознаками, що вказують на використання банку злочинними угрупованнями, є значні депозити готівкою, що швидко переводяться на інший рахунок, наявність рахунку, відкритого на юридичну особу, яка веде розрахунки готівкою, а не чеками чи акредитивами, переказ на рахунок значних «круглих» сум, депонування грошей на рахунок від різних людей, без видимої на те причини. Викликати підозру повинні також і часті перекази грошей без очевидної причини, компенсаційні кредити, часте об'єднання грошей з малих рахунків у великий, кошти з якого після чого перераховуються до іншого банку, або рахунок, на якому не провадяться

операції протягом значного періоду, після чого наступає період підвищеної активності, який потім переходить знову до періоду «сплячки».

Несподіване погашення «проблемного» кредиту є ознакою того, що його було використано для відмивання грошей, так само як і погашення кредиту, виданого третій стороні. Якщо клієнт завжди намагається мати справу з одним і тим самим співробітником банку, то це може вказувати на наявність «інсайдера». На це також вказує несподіване підвищення рівня добробуту окремого банківського працівника. Ділові структури, які не використовують банківських кредитів, інших видів сервісу з управління рахунками, є підозрілими як фіктивні.

Підставні фактури на імпорт-експорт та «подвійні фактури» – видані із завищенням реальної вартості товару, після сплати легалізують кошти, отримані злочинним шляхом. Завищення експорту дозволяє легалізувати кошти, отримані з-за кордону таким шляхом:

придбання майна чи монетарних засобів на кошти, отримані від злочинної діяльності. Матеріальне майно чи монетарні засоби купуються для подальшого перепродажу чи особистого збагачення. Для придбання різного роду активів широко використовуються зони вільної торгівлі. Набуте майно в подальшому може використовуватися для продовження незаконної діяльності (транспортні засоби, будинки). Переведення готівки у монетарні засоби полегшує переміщення грошей.

Широко використовуються для відмивання казино, зокрема, як підставні фірми. За оцінками Мережі боротьби з фінансовою злочинністю Казначейства Сполучених Штатів, загальний прибуток від 2000 найбільших казино у 130 країнах світу складає більше 30 млрд дол. США щорічно. Кримінальні структури купують право власності на такі установи для змішування коштів і їх подальшої легалізації. У казино готівка переводиться у фішки, програється мінімальна сума, після чого фішки переводяться назад у готівку, чек чи на банківський рахунок.

Перепродаж облігацій через підставних посередників відбувається у разі, якщо нова компанія здійснює випуск акцій, що скуповуються кримінальними елементами через офшорні агентства, після чого організовують їх продаж і отримують «відмиті» кошти.

Слід зазначити, що практично всі механізми «відмивання» коштів потребують значних витрат для тих, хто виконує такі операції. За оцінками фінансових експертів Інституту юридичних досліджень (Лондон), плата за відмивання коштів може досягати 30% від суми, що «відмивається».

Привабливими для «відмивання» грошей в першу чергу є офшорні зони, такі, як Кайманові острови, Кіпр та Панама, великі фінансові центри на зразок Сполучених Штатів, Великої Британії, Гонконгу та Сінгапуру, країни, в яких зберігається банківська анонімність, такі, як Ліхтенштейн,

Люксембург і донедавна Швейцарія, регіони із слабким валютним регулюванням на зразок Росії чи Східної Європи, а також із слабким законодавством та рівнем забезпечення правопорядку (Латинська Америка, Африка).

Світова практика вживання заходів щодо протидії «відмиванню» коштів має свій вираз у тенденції останнього часу у світовому розвитку правових систем, де настає поступове звуження розмежування між різними сферами законодавства. Найбільше це помітно у такій сфері, як фінансове регулювання. Це законодавство спрямоване в першу чергу на захист держави і суспільства, а не на узгодження взаємодії між юридичними особами, тому природним є його подальший розвиток у напряму заборон та санкцій, що є характерним для кримінального права. Наприклад, використання інформації, яка може відчутно впливати на ціну товару в разі, якщо цю інформацію отримано від «інсайдера», спрямоване на отримання зиску від торгівлі облігаціями певної корпорації, тобто зловживання службовим корпоративним становищем (insider dealing). Чи відноситься це до питань традиційно «корпоративного» права, що регулює діяльність юридичних та фізичних осіб на ринку, чи, беручи до уваги стурбованість більшості країн ринкової економіки діяльністю того роду, яка становить небезпеку для цілісності та функціонування відкритого ринку, до компетенції кримінального права? Це питання, окрім академічного, може становити і чисто практичний інтерес. Наприклад, в деяких країнах, зокрема у Сполучених Штатах, федеральне законодавство регламентує питання зловживання службовим корпоративним становищем, що стосуються міжнародної торгівлі та фінансів з метою захисту ринків, поза межами традиційного торгового права. З іншого боку, в правовій системі Канади така діяльність підпадає під компетенцію торгового права. Аналогічні питання постають в контексті визначення компетенції органів Європейського Союзу, а також компетенції органів окремих держав при проведенні реформування законодавства або правоохоронної системи.

У Британії до недавнього часу протидія зловживанню службовим корпоративним становищем як таким, що становить загрозу цілісності та функціонуванню національного ринку, відносилася до виключної компетенції кримінального законодавства. Така діяльність розцінювалася як серйозний злочин з 1980 р., і, незважаючи на те, що застосування кримінального законодавства у багатьох випадках є проблематичним, Комісія Палати представників виступала проти введення практики, яка дуже ефективно застосовується у Сполучених Штатах та передбачає вживання цивільно-правових заходів. Міністерство торгівлі Великої Британії наполягало на тому, що, оскільки така діяльність становить суспільну загрозу, вона підпадає під компетенцію кримінального

законодавства. Той факт, що система кримінального правосуддя виявилася малоефективною в боротьбі з серйозними економічними злочинами, не брався до уваги, оскільки суперечив «теорії права». Проте, 6 травня 1998 р. Голова секретаріату Казначейства зробив заяву, що уряд буде вводити законодавство, яке передбачатиме створення в Британії Фінансової служби, що буде вживати цивільно-правові заходи щодо фактів зловживання корпоративним службовим становищем.

Так само і контроль за відмиванням коштів становить інтерес для тих правників, хто займається комерційними та фінансовими секторами. Так, уряд Британії оголосив, що Фінансова служба буде займатися злочинами, пов'язаними з «відмиванням» коштів, хоча й матиме повноваження застосовувати лише цивільно-правові санкції. Таким чином, цей різновид злочинної діяльності можна розглядати як такий, що торкається широкого спектру правових питань.

Набуття та здійснення контролю над власністю є мотивом більшості умисних серйозних злочинів. Це тим більше стосується організованих кримінальних угруповань – «злочинних підприємств», що потребують значних коштів для забезпечення свого функціонування. Гроші, а швидше майно, у формі, що дозволяє вільно ним розпоряджатися, є не тільки метою організованих злочинних угруповань, а й життєвою потребою для «кримінальних підприємств». Таким чином, доти, доки гроші не будуть вилучені у злочинців, не можна говорити про ефективну протидію організованим злочинним угрупованням. Якщо держава вживає заходів щодо відслідковування та вилучення коштів, отриманих злочинним шляхом, кримінальні угруповання повинні, так чи інакше, ховати джерела своїх надходжень, тобто «відмивати» кошти.

Як і більшість соціальних та економічних явищ, «відмивання» коштів не є чимось новим. Воно так само старе, як і потреба ховати гроші від інших, і проблема використання прихованих коштів не є характерною лише для сьогодення. Зазвичай сучасні злочинці використовують більш досконалі прийоми, аніж перевізники-контрабандисти перлин з Індії чи лицарі тамплієри, але мета у них та сама – приховати джерело доходів, і таким чином, природу свого багатства. А виконується це за посередництвом низки трансакцій, реальних або фіктивних, направлених на те, щоб збити з пантелику особу чи орган, що провадить нагляд, і ускладнити розслідування.

Цілком очевидно, що ті, хто відслідковує переміщення майна, з метою його оподаткування, реституції чи конфіскації потребують допомоги тих, хто, умисно чи не умисно, бере участь у процесі «відмивання». Все це важким тягарем лягає на плечі тих, хто має справу з грошима інших осіб. Зараз на них покладається не лише облік трансакцій, але й проведення

відповідних дій з отримання інформації щодо походження коштів, а також природи окремих трансакцій. Законні та адміністративні акти, що їх мають виконувати банкіри та інші посередники, можуть передбачати серйозні правові наслідки в разі ухилення від інформування або недостатнього інформування.

Існує багато причин, чому особа або організація роблять спроби приховати джерело своїх надходжень, їх власника або характер. Значна увага приділяється тим вражаючим обсягам коштів, що надходять від наркобізнесу, хоча не слід забувати про те, що відмиватися можуть і кошти, отриманні від інших злочинів, і навіть кошти, набуті не кримінальним шляхом, але є потреба цей спосіб приховати. Потреба у «таємних грошах» існує не лише у синдикатів організованої злочинності, а й у розвідувальних мереж. У багатьох ситуаціях виникає потреба в «необлікованих коштах» і гроші, що відмиваються, утворюють приховані резерви «таємних коштів», які використовуються на потребу окремих осіб чи організацій. У разі застосування економічного ембарго щодо окремих країн, ними використовуються всі технічні прийоми, характерні для відмивання коштів, аби це ембарго обійти. Так само і політичні лідери окремих країн, що розвиваються, які намагаються вивезти капітал за межі своєї країни, коли це обмежується національним законодавством, використовують багато прийомів, характерних для злочинних угруповань, що намагаються легалізувати кримінальні прибутки. Хоча зазвичай, ставлення до них з боку фінансових інституцій значно різняться від такого до транснаціональних наркокартелів та міжнародних терористичних організацій.

Окремі країни намагаються залучити гроші в свою економіку, приваблюючи їх власників повною конфіденційністю як для них самих, так і для їх трансакцій. У деяких випадках гарантування конфіденційності розглядається як привабливий товар, який можна купити за досить помірковану ціну. В цьому випадку банкір не робить різниці між грошима, вивезеними біженцями з країни з репресивним режимом, витоком капіталу і «брудними» грішми. Багато країн є настільки ізольованими від традиційних джерел фінансів, що їх лідери просто не мають альтернативи і вимушені користуватися послугами тих, хто бажає схованки для своїх капіталів. Відмивання грошей через національні казначейства, різноманітні урядові проекти є звичайною справою для таких держав. З іншого боку, така практика може сприяти поширенню в цих країнах шахрайства і стосовно власних банкірів.

Під «брудними грошима» маються на увазі кошти, отриманні від злочинної діяльності. В широкому розумінні, гроші можуть не бути безпосереднім результатом злочинної дії, хоча може з'явитися потреба приховати їх джерело чи власника. Та навіть якщо не розглядати

взаємозв'язки, постає питання – які первинні дії є достатніми для того, щоб гроші можна було визначити як «брудні». Виключно кримінальний злочин, просто аморальна дія, адміністративне правопорушення тощо. Діяння, що розглядається як злочин в одній країні, може не бути таким в іншій, і, напевне, взагалі не буде братися до уваги в місці, де гроші знайдуть свій притулок, – офшорній зоні тощо.

Важливість цього питання стає очевидною, якщо розглянути значні кошти, які було отримано Коза-Нострою під час дії в США «сухого закону». Якби такий закон діяв зараз в Сполучених Штатах, і ці гроші було б переміщено до інших країн, то чи розглядалась би така діяльність як «відмивання коштів»? З точки зору США – так, але не з точки зору більшості інших країн. Навіть якщо гроші отримано від звичайного злочину, постає питання часу давності та наскільки важким він є в різних юрисдикціях.

«Відмивання» грошей – це процес, спрямований на приховання їх джерела. У зв'язку із тим, що більшість коштів, які відмиваються, надходять від наркобізнесу, питання боротьби з «відмиванням» грошей часто розглядається саме в цьому контексті. З погляду розробки законодавства та розвитку міжнародного співробітництва найбільш вагомі кроки зроблені саме у напрямі боротьби з «відмиванням» наркогрошей.

Найбільш широко дискусія щодо процесу «відмивання» має місце у Сполучених Штатах. Навіть звичайний процес «відмивання» передбачає низку акцій і не може розглядатися як безперервний. Він рідко обмежується лише заходами з ускладнення розслідування, що є характерним лише для справ, пов'язаних з шахрайством.

Як зазначалося вище, відмивання містить у собі кілька стадій і різні правові заходи можуть вживатися на кожній з них.

Багато форм злочинної діяльності призводять до появи значних сум грошей у дрібних купюрах. Виникає потреба перевести їх у форму, придатну для транспортування, зокрема за межі певної юрисдикції. Методи досягнення цієї мети обмежуються лише здібностями того, хто «відмиває». Звичайно, фірми з великим обігом та незначним інвестуванням є особливо привабливими, особливо якщо знаходяться поза межами традиційної банківської системи.

Коли гроші переведено у форму, придатну для транспортування, вони можуть бути переміщені до офшори. Це має кілька привабливих сторін. У першу чергу, кошти виходять за межі юрисдикції країни, де їх було набуто. Навіть, якщо закон має екстериторіальну силу, виникає низка бар'єрів щодо їх практичного застосування, зокрема обміну доказами, які можуть використовуватися у суді. Як вже зазначалося, окремі юрисдикції пропонують банківські та інші послуги, гарантуючи повну конфіденційність. Деякі країни умисно підготували свою систему для прийому

коштів з сумнівних джерел. З офшорної зони гроші можуть прямо чи побічно потрапити до звичайної банківської системи. Звичайно, чим більш дискретним є процес, тим краще для того, хто «відмиває». Таким чином, привабливими є юрисдикції, що прямо гарантують конфіденційність, або з таким рівнем корупції, що забезпечить відмову у співробітництві з правоохоронними органами інших країн.

Потрапивши до банківської системи, гроші можуть переміщуватися звичайними каналами. Метою стає формування складного «павутиння» трансакцій, через максимальну кількість юрисдикцій. Це робиться для ускладнення розслідування і встановлення шляху, яким йшли кошти. Беручи до уваги легкість, з якою юридичні особи утворюються по всьому світові, «відмивача» може обмежувати лише час та ресурси, що витрачаються.

З іншого боку, слід пам'ятати, що «відмивання» грошей не є безкоштовним, і той, хто «відмиває», так само як і його «боси», бажає витратити лише стільки, скільки реально потрібно для приховання грошей від правоохоронців та інших компетентних органів. Зрозуміло, що ресурси, які витрачатимуться на «відмивання» наркогрошей, будуть більшими від тих, що підуть на приховання хабара. Треба також враховувати, що доти, доки гроші знаходяться у процесі «відмивання», вони не можуть бути використані. Таким чином, злочинець зацікавлений не лише у зменшенні вартості «відмивання», а й у скороченні часу, що витрачається. Враховуючи важливість максимального зменшення записів та іншої документації, серед «відмивачів» поширюється тенденція до повернення до старої практики контрабанди готівки. Контейнерні перевезення є найзручнішим для цього засобом, оскільки дозволяють направити готівку у значній кількості до будь-якої країни без відповідних записів.

Обставини, зазвичай, впливають на процес «відмивання», що може складатися як з простих маніпуляцій рахунками, так і зі складного процесу, до якого залучаються сотні компаній та тисячі банківських рахунків. У той же час, чим більша організація, тим більша ціна, ризик виявлення та інших негативних наслідків.

Трансакції, направлені на приховування джерел коштів, структуруються таким чином, що отримання доказів для суду стає практично неможливим. Мається на увазі розглянута вище стадія розшарування. Хоч у деяких випадках вдається в ході розслідування підняти кілька шарів, через які проводилися гроші, і навіть виявити першоджерело, сама концепція «розшарування» є, до певної міри, спрощенням. Операції часто нагадують скоріше мозаїку калейдоскопу, аніж шари у торті. Трансакції слідують не одна за одною, а паралельно, угоди об'єднуються та роз'єднуються. Найвразливішим є момент, коли гроші потрапляють до банківської

системи, – саме тоді регуляційні правила, що вимагають проведення фінансовим сектором відповідної перевірки, є найефективнішими.

За останні роки багато уваги приділяється використанню новітніх технологій за відмивання коштів. Немає сумнівів, що кримінальні структури повною мірою користуються перевагами технічного прогресу, зокрема в сфері телекомунікацій. В першу чергу, йдеться про системи електронного зв'язку, мережі «Інтернет», мобільні телефонні комунікації.

Коли гроші, до задоволення «відмивача», перемішані, самий час розмістити їх у потрібному місці, тобто зробити «остаточний депозит». Вибір такого місця зазвичай залежить від низки факторів. У багатьох випадках бажано повернути кошти туди, де їх було отримано. Зокрема, діюча протягом тривалого часу кримінальна структура, через яку гроші було отримано, потребує свого фінансування. З цією метою провадиться одна або, швидше, низка трансакцій з переміщення вже «чистих» грошей. Це може бути зроблено багатьма способами, основною вимогою до яких є те, що вони повинні мати правдоподібне пояснення.

Ефективною технікою тут є утворення підставних фірм, які «продають» свої облігації «закордонному інвестору». Придбання таких облігацій належним чином документується, і гроші попадають в розпорядження тих, хто ініціював процес. При розслідуванні справ з «відмиванням» коштів не завжди вдається ідентифікувати такі операції, – інколи їх сприймають як шахрайство.

Таким чином, кожна стадія в процесі «відмивання» коштів має власні характеристики. Законодавці не завжди можуть усвідомити складність процесу «відмивання» грошей. Наприклад, такого феномену, як зазначена вище підпільна банківська система.

Інтерес становить не лише сам процес «відмивання», а й люди, причетні до цього, – готові за відповідну платню або частку надати відповідні послуги тим, кому потрібно свої гроші «відмити» або приховати. Недавні розслідування, що провадилися Митною службою Великої Британії, викрили мережу осіб, які обслуговували фінансові інтереси терористів з Північної Ірландії, грабіжників банків в Англії, розповсюджувачів наркотиків з Майамі та шахраїв з Гонконгу за допомогою одного офшорного банку на Карибах. Одна з цих осіб мала дипломатичний статус. Багато з них є експертами з фінансових питань та цивільного права і створили мережу компаній та інших юридичних осіб в юрисдикції, про яку не відомо, щоб вона мала бажання чи можливості із забезпечення правового режиму. В ході розслідування викрито факти, що вказували не лише на їх готовність до участі у «відмиванні» грошей, а й до проведення будь-яких сумнівних фінансових та інших комерційних трансакцій. Зокрема, юридичні особи, що знаходилися під їх контролем, використовувалися в ролі підставних,

надавалася допомога при проведенні шахрайських акцій і т. ін. Таким чином, сучасний «відмивач» рідко коли буває членом кримінальних структур, швидше він буде на периферії фінансового сектору чи банківської індустрії або є професійним консультантом, юристом чи бухгалтером, готовим надавати послуги будь-кому, хто готовий платити. (Схему «відмивання» грошей з конвертуванням у ВКВ подано у табл. 5)

Беручи до уваги занепокоєність більшості країн проблемою наркобізнесу, не дивно, що вони мають значну кількість законодавчих актів та інших правових норм, присвячених боротьбі з «відмиванням» коштів, отриманих від наркозлочинів та інших форм оргзлочинності. Переважна більшість цих норм права передбачає конфіскацію коштів, щодо яких доказано, що вони, так чи інакше, походять від серйозних злочинів.

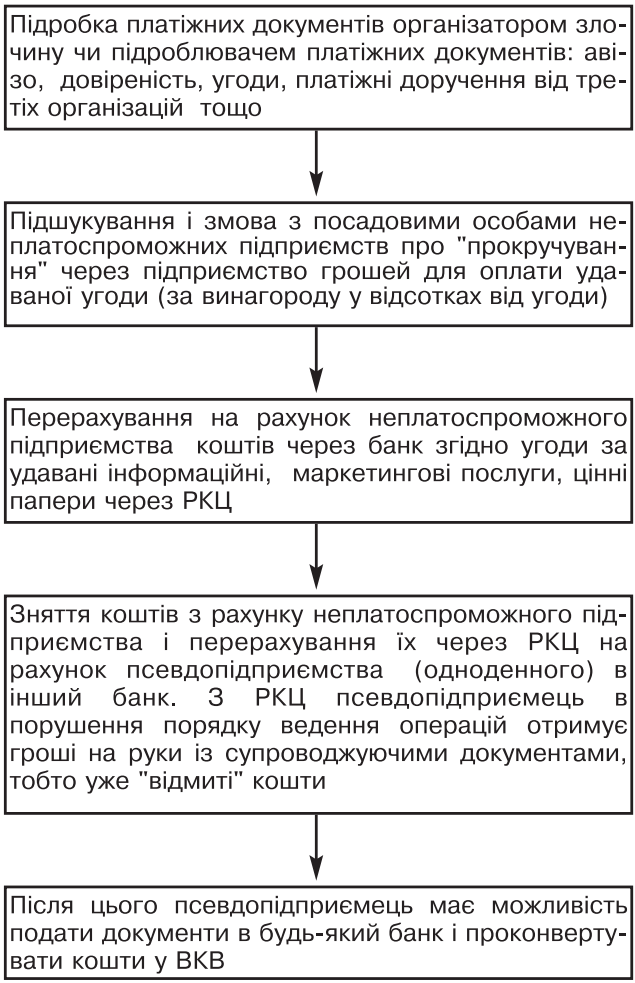
Насправді ж ці нові закони, що стали відповіддю на збільшення випадків відмивання, скоріше лякають можливістю, ніж застосовуються на практиці.

Визначення ефективності конфіскаційного законодавства є надзвичайно складним. Зазвичай застосування будь-якої юридичної процедури може бути оцінено на ефективність, але при цьому також слід враховувати той вплив, який вона має на діяльність проти якої спрямована, що потребує проведення оцінки цієї діяльності. Сума, яка надходить від торгівлі наркотиками, інших видів злочинної діяльності, залишається вельми приблизною. Країни «третього світу» та ті, що змінюють свою економіку з державно-колективістської на ринкову, мають значну частину підпільної та тіньової економіки. Це також ускладнює аналіз. За останніми оцінками через фінансовий сектор США щороку відмивається 500 млрд доларів, а через фінансові інституції лондонського Сіті – 200 млрд фіктивних структур (ф.с.). В той же час, з 1986 р., коли в Британії було введено нове конфіскаційне законодавство щодо грошей, що «відмиваються», вилучено було лише 40 млн ф.с. Тобто дуже приблизно держава змогла вилучити лише 0,002 % кримінальних грошей, що проходять через Лондон. За оцінками тих самих британських експертів у 1997 р. всього в світі конфісковано 250 млн ф.с., більша частина з яких припадає на США. За оцінкою деяких представників уряду США, щорічно у світі відмивається близько 3 трлн доларів.

У Києві розкрито розгалужену мережу фіктивних структур, через яку проводилося «відмивання» «тіньових» коштів. Тільки за період з серпня 2001 р. до лютого 2002 р. через цю мережу було «відмито» і легалізовано 196,9 млн грн. Активним учасником протиправної діяльності було дочірнє литовське приватне підприємство [162, с. 3].

Таблиця 5

Схема «відмивання» грошей з їх конвертуванням у ВКВ



На сьогодні в світі є небагато країн, в яких відсутнє законодавство щодо «відмивання» грошей, що надходять від контрабанди наркотиків, і в яких не криміналізовано спроби «відмивання» таких прибутків. Проекти таких законів розроблялися у міжнародних організаціях і відображають тенденції в світі щодо захисту суспільства від міжнародної організованої злочинності. Можливо є ті, хто пропагує ці закони і вірить в їх ефективність, але факти

свідчать, що вони мають лише дуже незначний вплив як на злочинців, так і на їх структури.

Закони по боротьбі з «відмиванням» грошей, що впроваджуються в різних країнах, оперують на трьох рівнях. По-перше, вони накладають певні обов'язки на осіб, котрі мають справу з грошима інших людей – проводити записи і звітувати стосовно трансакцій, що перевищують певну суму. Це законодавство спрямовано на виявлення «відмивання» грошей, коли останні потрапляють або знаходяться у фінансовій системі. По-друге, закони передбачають кримінальну відповідальність за сприяння процесу «відмивання», усвідомлюючи чи маючи підозру, що власність набуто шляхом вчинення злочину. По-третє, низка обов'язків покладається на осіб, що регулярно мають справу з грошима інших осіб. Зазвичай вони повинні знати своїх клієнтів, належним чином реєструвати трансакції і до певної міри вживати заходів стосовно з'ясування природи трансакцій. Ці правові акти підкріплюються іншими законами та регуляційними правилами.

Окрім внутрішніх ініціатив існує низка міжнародних проектів, спрямованих на вдосконалення взаємодії та сприяння проведенню спільних розслідувань. У національних законах з цього питання зазначається можливість проведення розслідування за інформацією від інших країн.

Не зважаючи на все, інформація, зокрема від розвідувальних структур, які починають відігравати все більшу роль у процесі протидії цьому явищу, вказує, що війна проти «відмивання» коштів програється. Традиційна система кримінального законодавства, на якій базується більшість законодавчих ініціатив з порушеного питання, виявляється малоефективною. Кримінальне законодавство і структури, що мають забезпечувати його ефективне функціонування, зокрема судові органи, виявляються неефективними при розслідуванні серйозних фінансових злочинів.

У Сполучених Штатах Америки та кількох інших юрисдикціях для вилучення прибутків від злочинної діяльності використовується не лише кримінальне, а й цивільне законодавство, а також адміністративні процедури. Зокрема, цивільне законодавство використовується для вдосконалення системи звітності щодо підозрілих трансакцій. І хоча ці правові норми розроблялися для системи, що діє в США, і базуються вони на англосаксонському праві, деякі їх базові принципи можуть становити інтерес і для систем континентального права.

З цілої низки справ британські суди накладали цивільні санкції на осіб, причетних до «відмивання» коштів. Ця практика починає поширюватися серед інших країн саксонської правової системи, і є багато ознак, що у майбутньому вона буде застосовуватися і в юрисдикціях континентальної системи.

На думку багатьох західних юристів, закони і процедури, що покладаються на потребу встановлення зв'язку між злочином та майном, приречені бути недієвими. У кримінальному судочинстві немає і ніколи не буде ресурсів, які могли б бути виділені на встановлення зв'язків за стандартом, необхідним для судового розгляду кримінальної справи. Законодавство з «відмивання» коштів повинно використовувати механізми, що застосовуються у антикорупційному законодавстві окремих країн, за яким відповідальність за пояснення походження коштів у певних ситуаціях, покладається на власника. Ця процедура має багато схожого із системою, яка використовується податковими органами. Згідно із Актом щодо контролю за доходами від злочинної діяльності 1995 р. (Велика Британія), два засудження за серйозні злочини протягом шести років створюють презумпцію того, що власність особи отримана злочинним шляхом. У цьому разі тягар доказування законності набуття коштів перекладається на звинуваченого.

Згідно із діючим в Італії законодавством (Закон № 646 1982 р.) для встановлення того, чи отримано власність від злочинної дії, можуть застосовуватися два методи. Згідно із першим, перевіряється законність джерела доходів через отримання доказів, що свідчили б про можливу причетність особи до злочинної діяльності. Подальший розгляд справи проводиться в межах традиційного кримінального судового провадження.

Згідно із другим методом, що базується на принципах цивільного права, встановлюється власність, законний характер якої викликає сумнів у зв'язку з швидкістю її придбання, великою цінністю, наявністю доказів проти власника. Після проведення оцінки власності та збирання інформації, що стосуються справи, від власника вимагається надання доказів законного походження власності. Прокурор чи квестор перевіряють спосіб життя, масштаби доходів, оцінюють рухоме та нерухоме майно, факти щодо його можливої участі в господарських операціях, виявляють диспропорції між офіційними та реальними доходами. Об'єкт має довести законність джерела своєї власності. В іншому випадку власність може бути конфісковано і передано державі без проведення кримінального процесу.

За наявності зв'язків особи з організованою злочинністю, Закон № 646 презумує незаконний характер збагачення і вимагає від особи, що знаходиться під підозрою, надати докази протилежного. Подібні обов'язки покладаються і на зв'язки особи, які могли б використовуватися для приховування капіталу. Такий механізм не стосується сфери застосування кримінальних санкцій, і, таким чином, вважається, що він не суперечить принципу презумпції невинуватості. Право на захист при цьому гарантується. Якщо власник доведе законний характер походження майна, винесена заборона на користування цією власністю відміняється. На думку

італійських правників, наведений метод є ефективним для руйнування економічної бази організованої злочинності, повернення державі коштів, отриманих від незаконної діяльності.

Закон № 646 1982 р. надає компетентним органам право перевірки фінансового становища членів родини та інших осіб, що проживали разом із особою, на яку впала підозра, протягом останніх п'яти років. Зазначені особи повинні довести, коли і яким чином вони стали власниками певного майна. Для розслідування та встановлення випадків незаконного збагачення податкова поліція має повноваження витребувати, без попереднього рішення суду, інформацію у кредитних установ, вивчати банківські документи і т. ін.

Протягом останніх років у Швейцарії введено в дію відповідне законодавство, спрямоване на боротьбу з «відмиванням» грошей. Значно обмежено можливості дотримання банківської таємниці, розширено взаємодію з партнерами з інших країн при проведенні розслідування.

Однією з основних ланок швейцарської системи є зберігання документів щодо економічних прав з метою недопущення анонімності. Конвенцією щодо обачності банків від 1 липня 1992 р. передбачено встановлення особи клієнта, перевірку відомостей щодо сторін у договорі та власників майнових прав. Згідно із проектом Федерального закону Швейцарії щодо «відмивання» грошей від 1994 р., ці вимоги розширено на весь фінансовий сектор, що має сприяти встановленню внутрішніх правил поведінки, і на фінансових посередників небанківського сектору.

При відкритті рахунку, отриманні ощадної книжки, оренді сейфа, клієнт зобов'язаний пред'явити документ, що підтверджував би особу, – паспорт для фізичних осіб, виписку із Торговельного реєстру для юридичних осіб. Банк або інша фінансова установа повинна вести реєстр імен, прізвищ, дат народження, громадянства та адреси фізичних осіб, назв та офіційні адреси юридичних осіб.

Банк перевіряє і «випадкових» клієнтів, наприклад осіб, що проводять обмін валюти на суму, що перебільшує 25 тис. швейцарських франків. Якщо сума достатньо велика, то перевіряються не лише дані щодо клієнта, а й вимагається підтвердження права на економічні права. Подібний контроль передбачено і у разі, якщо провадиться низка трансакцій на загальну суму, що перебільшує визначений мінімум.

На фінансові установи покладено обов'язок провадити перевірку не лише щодо клієнта, а й щодо реального власника економічних прав, в першу чергу можливих беніфіціаріїв. Встановлення даних стосовно клієнтів є обов'язковим і у випадку, коли обсяг трансакцій менший за встановлений мінімум, але існують ознаки, які вказують на те, що має місце «відмивання» грошей.

Закон зобов'язує провадитити перевірку відомостей щодо власника економічних прав, котрий не є стороною в договорі, коли є дані, що така сторона не є власником коштів, стосовно яких має місце угода, або щодо цього є сумніви. У цьому випадку від сторін вимагається не лише підтвердження даних, але й підтвердження права власності або вказівки на справжнього власника. Отримані дані заносяться до відповідного реєстру.

Якщо ділові стосунки встановлено шляхом листування або якщо провадиться достатньо значна операція, перевірка права власності є обов'язковою.

Коли стороною є юридична особа, слід отримати дані щодо того, хто її очолює. Якщо власника не визначено, отримуються дані щодо всіх осіб-керівників.

Згідно зі ст.7 Закону РФ «Про протидію легалізації («відмиванню») доходів, отриманих злочинним шляхом» організації, які провадять операції з грошовими коштами та іншим майном, повинні подавати в уповноважений орган інформацію про операції, які підлягають обов'язковому контролю. Вони повинні документально фіксувати інформацію у таких випадках: заплутаний або незвичний характер правочину, який не має очевидного економічного змісту, або очевидної законної мети; невідповідність правочину цілям діяльності організації її установчим документам; виявлення неодноразового вчинення операцій або правочинів, характер яких дає підстави вважати, що метою їх проведення є ухилення від процедури обов'язкового контролю, інші обставини, які дають підстави вважати, що правочини вчиняються з метою легалізації доходів, отриманих злочинним шляхом.

Конфіскація майна є не менш, а інколи і більш дієвим засобом боротьби зі злочинністю, ніж арешт та засудження до позбавлення волі. Уникнувши вилучення, злочинці продовжують кримінальну діяльність, навіть перебуваючи в місцях позбавлення волі. «Що турбує нас більш за все, так це те, коли ви забираєте у нас гроші. Краще сидіти у в'язниці та зберегти гроші, ніж бути на свободі без грошей», – казав Гаспаре Мутоло, один з провідних «діячів» італійської мафії.

Відповідно до проектів Закону України «Про боротьбу з легалізацією доходів, отриманих злочинним шляхом», право власності не розповсюджується на кошти та майно, отримані від злочинної діяльності. В той же час, механізм вилучення таких коштів не визначено. В окремих країнах, зокрема у Сполучених Штатах Америки, для вилучення коштів від злочинної діяльності, використовуються два види конфіскації – кримінальна та цивільна. Кримінальна конфіскація, як і в Україні, провадиться в межах кримінального процесу, але відмінністю американської системи є

те, що конфіскуються лише кошти, отримані злочинним шляхом, – конфіскація як засіб покарання там не використовується. Таким чином, суд повинен довести, що кошти чи майно отримані саме від злочину, або використовувались при проведенні злочинної дії. Так, конфіскуючи транспортний засіб у особи, засудженої за контрабанду наркотиків, суд має довести, що вказана річ використовувалася для їх незаконного переміщення.

Що ж стосується цивільної конфіскації майна, то в цьому разі об'єктом справи є не особа, а саме майно. Справу може бути порушено і без порушення кримінальної справи проти власника. Це застосовується, зокрема, за відсутності складу злочину, якщо звинувачений помер і т. ін. Юридична теорія при цьому стверджує, що закон порушила не особа, а майно, що сприяло злочину чи отримане від нього. Фактично суд визначає правомірність права власності.

Позивач (тобто уряд) повинен продемонструвати достатні підстави того, що право власності на майно є недійсним. До позову може додаватися свідчення під присягою, що його дав співробітник правоохоронних органів, який арештував майно.

Після того, як надані достатні підстави, тягар лягає на плечі потенційного позивача. Позивач повинен довести, що він має право власності на таке майно. Загалом, розгляд зазначеної справи складається із таких стадій:

– слідство до арешту, що включає встановлення достатніх підстав, можливості позову невинного власника;

– арешт, що провадиться на підставі ордера на арешт;

– зберігання та оцінка заарештованого майна;

– направлення потенційному позивачеві повідомлення про арешт, що включає також публікацію в місцевій газеті протягом трьох тижнів; повідомлення містить інформацію щодо арешту, порядку опротестування та про право на прискорене звільнення;

– прискорене звільнення має місце, коли подається клопотання про таке звільнення; рішення щодо цього приймається прокурором;

– рішення про конфіскацію приймається у разі дефолту, тобто якщо не подано позов про звільнення протягом 10 діб з часу отримання повідомлення, або якщо позов подано, але не дано відповіді на звинувачення протягом 20 діб та на підставі рішення, прийнятого в порядку спрощеного судочинства проти майна та всіх існуючих потенційних позивачів, якщо позивачі не можуть довести наявність достовірних істотних фактів по суті своїх позовів;

– представлення документів в суд відбувається у разі, якщо позивачі не дали відповідь на звинувачення і довели наявність достовірних істотних

фактів по суті свого позову, справа проходить етапи процесу, включаючи обопільне представлення документів, дачу свідчень, судові клопотання і розгляд; якщо уряд має перевагу, виноситься рішення про вилучення майна (тобто проти майна) і відхилення позовів;

– федеральний прокурор може санкціонувати задоволення вимог позивача шляхом повного звільнення від конфіскації або шляхом пом'якшення санкцій, тобто часткового задоволення вимог;

– кінцевий етап – відчуження конфіскованого майна шляхом переведення грошей з рахунку, призначеного для зберігання, у конфіскаційний фонд або передача негрошового майна у державну власність, зокрема шляхом його продажу.

Інколи під час цивільної конфіскації використовуються адміністративні процедури замість судових. Це має місце, наприклад, щодо майна вартістю не більше 500000 доларів США, транспортних засобів, що використовувалися для перевезення контрабанди, та монетарних засобів (готівки та цінних паперів).

Після арешту майна орган, що його провадив, повідомляє зацікавлених фізичних та юридичних осіб (потенційних позивачів) про намір конфіскації. Для опротестування арешту позивач повинен надіслати поштою позов. У разі опротестування адміністративного арешту орган, що його провів, має передати справу Федеральному прокурору для порушення судової справи про цивільну конфіскацію.

Цивільні адміністративні процедури займають від трьох до п'яти місяців. При цьому виконуються такі кроки:

– слідство до арешту – встановлення достатніх підстав, оцінка та визначення правового статусу;

– арешт на підставі ордера або без ордера;

– зберігання та оцінка заарештованого майна;

– повідомлення про арешт потенційних позивачів, а також через публікацію в газеті протягом трьох тижнів; повідомлення містить інформацію про намір провести конфіскацію, порядок опротестування арешту, щодо прискореного звільнення;

– прискорене звільнення має місце, як і при судовому розгляді;

– постанова про конфіскацію виноситься за відсутності позову або за відсутності клопотання про судовий розгляд; постанова виноситься керівником органу, що проводить конфіскацію;

– звільнення або пом'якшення має місце тоді, коли за клопотанням про звільнення від конфіскації або її пом'якшення керівник задовольняє такі вимоги чи шляхом повного звільнення від конфіскації, або шляхом часткового задоволення;

– відчуження майна має місце так само, як і за судового розгляду.

Таким чином, згідно із правовою доктриною США, цивільна конфіскація є судочинством проти майна (in rem), тоді, як кримінальна конфіскація є судочинством проти особи (in personem), якій інкримінується вчинення злочину. Фактично ж як кримінальна, так і судова конфіскація в США оспорюють право власності особи на певні речі, але різними шляхами. При кримінальній конфіскації уряд повинен поза всякими сумнівами довести, що звинувачений вчинив злочин за стандартом значно вищим, ніж достатня підстава у цивільному законодавстві, а також за досить високим стандартом (щоправда, нижчим, ніж поза всякими сумнівами), що майно набуто злочинним шляхом або використовувалося для вчинення злочину.

У цьому зв'язку викликає інтерес доктрина зворотної сили, за якою право власності на майно, що підлягає конфіскації, переходить до уряду тоді, коли була виконана дія, яка стала причиною конфіскації.

Законом передбачається захист особи, котра невинна у правопорушеннях, пов'язаних із майном. Як правило, особа має право на захист як законний власник, якщо вона не знала про незаконну діяльність, не погоджувалася на незаконну діяльність, не могла знати про незаконну діяльність або виконала всі в розумних рамках можливі кроки для відвернення незаконної діяльності. Залежно від прав невинного власника, конфіскацію буде анульовано або вартість, на яку поширюються права невинного власника, буде йому виплачена після конфіскації та продажу майна.

Особа, що заявляє про свої права невинного власника, має підтвердити заяву вагомими доказами.

Після того, як майно заарештовано, воно переходить у розпорядження судових виконавців. Заарештовані грошові кошти повинні бути переведені у депозитний фонд заарештованих активів протягом 60 діб після накладання арешту. Заарештоване майно не може використовуватися до підтвердження конфіскації. У тому випадку, коли майно не є грошовими коштами, потрібне також схвалення офіційного використання.

Все майно конфіскується або на підставі підтвердження за відсутності позову, або за рішенням суду. Після конфіскації майно може бути використане залежно від його типу та призначення. Конфісковані грошові кошти кладуться на рахунок служби, що провадила арешт, або у фонд конфіскованих активів Міністерства юстиції. Будь-яке інше майно, яке призначається для офіційного користування, тобто літаки, судна, будинки, автомобілі і т.ін., передається у таке користування, якщо воно відповідає певним вимогам. Інше майно продається, дохід від продажу передається до фонду конфіскованих активів.

Як свідчить світовий досвід, законодавча база з питань боротьби з «відмиванням» грошей має базуватися на таких основних принципах:

– криміналізація відмивання коштів дозволяє інкримінувати «відмивання» як злочинної діяльності;

– вдосконалення законодавства з питань припинення права власності, причому доцільним є впровадження саме цивільно-правової відповідальності за володіння коштами, отриманими від незаконної діяльності;

– реалізація системи з інформування відповідного регуляційного органу щодо трансакцій, що викликають підозру; це вимагає впровадження системи активного співробітництва між фінансовим сектором і державним регуляційним органом;

– впровадження системи контролю за грошовими переказами за кордон і з-за кордону;

– обмеження банківської таємниці, доступ до банківських рахунків з відповідної санкції суду, ліквідація анонімних та «номерних» рахунків.

Що стосується цивільно-правового боку такого законодавства, то він має передбачувати:

– визнання правочинів, які укладаються щодо фінансових засобів, майна чи майнових прав, що є доходом від злочинної діяльності, недійсними із настанням наслідків недійсних угод, які провадяться з метою, що суперечить інтересам суспільства та держави;

– покладання на громадян, котрі укладають майнові договори, провадять операції з фінансовими засобами, майном та майновими правами на суму, що перебільшує окремий, встановлений законом, мінімум, та/або за певних обставин, що вказують на можливий протиправний характер набуття майна, відповідальності за підтвердження законності їх походження.

31 березня 2000 р. Президент України підписав Указ «Про заходи легалізації фізичними особами доходів, з яких не сплачено податки», за ним повинно бути запроваджено одноразовий захід, коли слід подати декларацію у податкову службу без зазначення джерел походження коштів. Проміжок часу обмежено лише датою заповнення декларації. Фізичні особи в свою чергу звільняються від передбаченої чинним законодавством відповідальності, а легалізовані доходи у майбутньому не підлягають конфіскації. Посадові особи кредитно-фінансових, банківських установ, а також органів державної влади зобов'язані зберігати таємницю щодо інформації про легалізовані доходи.

Цей указ має на меті поліпшення інвестиційного клімату, розвитку підприємництва, залучення коштів з тіньового грошового обігу, а також поповнення кредитних ресурсів та спрямування їх в реальну економіку.

Починаючи з 2003 р. НБУ повів нещадну боротьбу з «брудними» грошима. Зокрема, закрив дві схеми вивозу капіталу за кордон – стосовно

подвійного викупу акцій та завищення цін і експорту фіктивних послуг. До кінця року планувалося перейти на міжнародні стандарти аудиту, щоб поліпшити інвестиційну привабливість вітчизняної економіки [160, с. 87].

З метою удосконалення законодавства з питань запобігання легалізації (відмивання) доходів, одержаних злочинним шляхом, та приведення деяких законів України у відповідність із Законом України «Про запобігання та протидію легалізації («відмиванню») доходів, одержаних злочинним шляхом», а також недопущення використання банків та інших фінансових установ з метою легалізації («відмивання») доходів, одержаних злочинним шляхом, та фінансування тероризму Верховна Рада України прийняла Закон «Про внесення змін до деяких законів України з питань запобігання використанню банків та інших фінансових установ з метою легалізації («відмивання») доходів, одержаних злочинним шляхом», затверджений Президентом України 6 лютого 2003 р.

Згідно із цими змінами банки зобов'язані розробляти, впроваджувати та постійно поновлювати правила внутрішнього фінансового моніторингу та програми його проведення з урахуванням вимог законодавства про запобігання легалізації («відмиванню») доходів, одержаних злочинним шляхом.

Національний банк України у процесі нагляду за діяльністю банків не рідше одного разу на рік проводить перевірку банків з питань дотримання ними законодавства, яке регулює відносини у сфері запобігання легалізації («відмиванню») доходів, одержаних злочинним шляхом.

Банк зобов'язаний ідентифікувати клієнтів відповідно до законодавства України.

Діяльність партій, рухів та інших громадських об'єднань, що мають політичні цілі, в Уповноваженому органі забороняється.

Абзац другий ч. 1 ст. 306 КК України викладено в такій редакції: «караються позбавленням волі на строк від п'яти до дванадцяти років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років з конфіскацією коштів або іншого майна, одержаних злочинним шляхом, та з конфіскацією майна».

Відповідно до ч. 1 статті 64 Закону України «Про банки і банківську діяльність» банкам забороняється вступати в договірні відносини з анонімними особами.

Продаж ощадних (депозитних) сертифікатів на пред'явника за готівку на суму, що перевищує еквівалент 10000 євро за офіційним курсом гривні до іноземної валюти, встановлений Національним банком України, або якщо ця операція має сумнівний характер, може проводитися щодо осіб, якщо вони нададуть документ, що засвідчує особу.

Згідно із ч. 3 ст. 64 Закону значними є операції, якщо безготівкові розрахунки за угодами провадяться на суми, що перевищують еквівалент 50000 євро, або угоди з готівкою на суму, що перевищує еквівалент 10000 євро за офіційним курсом гривні до іноземної валюти, встановлений Національним банком України. При цьому мається на увазі одноразове перерахування зазначених сум відповідно до угоди. Однак слід мати на увазі, що при перерахуванні суми, меншої за зазначену в ч. 3 ст. 64 Закону, але за угодою, що явно пов'язана з іншою угодою і загальна сума перерахування за цими угодами перевищує відповідно 50000 євро або 10000 євро, банки також зобов'язані ідентифікувати осіб, які провадять такі операції.

Національний банк листом від 19 квітня 2001 р. № 18-112/1467-2599 (або додаток В.33. с.118-129) відносить операції до таких, що потребують окремої уваги, мають такі ознаки:

1) операції з готівкою провадяться регулярно, іноді кілька разів на день;

2) частий обмін великої кількості купюр низького номіналу на купюри більшого номіналу;

3) угоди з готівкою на значну суму провадяться явно на користь третіх осіб;

4) розміщення на рахунку значної суми готівкових коштів клієнтом, який за рівнем доходів чи сферою діяльності не може провадити операцію на цю суму;

5) перетворення готівкових коштів у банківські чеки, переведення грошей в інші платіжні засоби;

6) розміщення та зняття готівкових коштів клієнтом, який зазвичайно оплачує чеками, переказами;

7) стрімке збільшення вкладів клієнта за рахунок внесення на цей рахунок готівкових коштів, з подальшим переказом цих коштів особі, яка не пов'язана з клієнтом комерційними відносинами;

8) переказ великих сум готівкових коштів за кордон з вимогою видати кошти одержувачу готівкою;

9) на рахунок клієнта провадяться перекази значних коштів за оплату робіт, надання послуг тощо, які не мають відношення до діяльності клієнта;

10) інкасація чека на значну суму, який виданий іноземним банком на пред'явника;

11) розміщення на щойно відкритий рахунок значної суми коштів;

12) зарахування на рахунок (вклад) готівки в упаковці, що опечатана іншим банком;

13) відкриття клієнтом рахунку в банку, на який протягом дня надходять кошти від багатьох комерційних структур, що різними способами

переводяться у готівку або на інший рахунок, в результаті чого на цьому рахунку на кінець дня не залишається коштів;

14) зарахування та/або списання коштів у значних сумах юридичною особою, операції за рахунках якої є незначними, або нещодавно створеною юридичною особою;

15) надходження іноземної валюти на рахунок юридичної особи за зовнішньоекономічними контрактами, які фактично цією юридичною особою не виконуються;

16) зарахування на рахунок грошових коштів, які надійшли від юридичної (фізичної) особи, яка знаходиться (проживає) та/або є власником рахунку в банку, який зареєстрований в офшорних або вільних економічних зонах, а так само в регіонах з нестабільною політичною, економічною ситуацією або пов'язаних з виробництвом наркотичних засобів; при цьому одержувач коштів не має з цією особою стійких комерційних контактів;

17) зняття з рахунку або зарахування на рахунок юридичної особи грошових коштів у готівковій формі у випадках, коли це не співвідноситься з характером діяльності цієї юридичної особи;

18) отримання фізичною особою грошових коштів на пред'явника, виданому нерезидентом, або за чеком, сума якого оголошена як виграш;

19) перерахування за кордон грошових коштів в іноземній валюті в сумі понад 100 тис. доларів США одноразово або протягом короткого часу (до 10 діб);

20)проведення операцій, за якими один і той самий фінансовий інструмент багаторазово продається і викупається за угодами з однією і тією самою установою.

Зазначений вище перелік не є вичерпним. У кожній конкретній ситуації банки повинні виходити з того, чи відповідає характер цієї операції її кінцевим результатам, а також чи існує зв'язок між операцією та характером діяльності, фінансовим становищем клієнта, враховувати регулярність проведення ним операцій за рахунком.

Але всі ці вимоги не є остаточними, оскільки Закон України «Про запобігання та протидію легалізації («відмиванню») доходів, одержаних злочинним шляхом» у ст. 11 наводить свій перелік фінансових операцій, що підлягають обов'язковому фінансовому моніторингу, на який, до речі, й орієнтуються банки у своїй діяльності. Фінансова операція підлягає обов'язковому фінансовому моніторингу, якщо сума, на яку вона провадиться, дорівнює чи перевищує 80000 гривень або дорівнює чи перевищує суму в іноземній валюті, еквівалентну 80000 гривень, та має одну або більше ознак, визначених цією статтею (Абзац перший ст. 11 зі змінами, внесеними згідно з Законом від 06 лютого 2003 р. № 485-IV):

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

купівля (продаж) чеків, дорожніх чеків або інших подібних платіжних засобів за готівку;

зарахування або переказ грошових коштів, надання або отримання кредиту (позики), проведення фінансових операцій з цінними паперами у випадку, коли хоча б одна із сторін є фізичною або юридичною особою, що має відповідну реєстрацію, місце проживання чи місце знаходження в країні (на території), яка не бере участь в міжнародному співробітництві у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, та фінансуванню тероризму, або однією з сторін є особа, що має рахунок в банку, зареєстрованому у зазначеній вище країні (на зазначеній вище території). Перелік таких країн (територій) визначається відповідно до порядку, встановленого Кабінетом Міністрів України на основі переліків, затверджених міжнародними організаціями, діяльність яких направлена на протидію легалізації («відмиванню») доходів, одержаних злочинним шляхом, та фінансуванню тероризму, і підлягає опублікуванню;

переказ коштів у готівковій формі за кордон з вимогою видати одержувачу кошти готівкою;

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

зарахування грошових коштів на рахунок чи списання грошових коштів з рахунку юридичної особи, період діяльності якої не перевищує трьох місяців з дня її реєстрації, або зарахування грошових коштів на рахунок чи списання грошових коштів з рахунку юридичної особи у випадку, якщо операції на зазначеному рахунку не проводилися з моменту його відкриття;

відкриття рахунку з внесенням на нього коштів на користь третьої особи;

переказ особою, за відсутності зовнішньоекономічного контракту, коштів за кордон;

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

проведення фінансових операцій з цінними паперами на пред'явника, не розміщеними в депозитаріях;

придбання особою цінних паперів за готівку;

виплата фізичній особі страхового відшкодування або отримання страхової премії;

виплата особі виграшу в лотерею, казино або в іншому гральному закладі;

розміщення дорогоцінних металів, дорогоцінного каміння та інших цінностей в ломбарді.

Оскільки Законом України «Про організаційно-правові основи боротьби з організованою злочинністю» не визначений механізм надання банками інформації, передбаченої ч. 6 ст. 64 Закону, банки надають інформацію щодо проведення їх клієнтами значних та/або сумнівних операції у довільній формі спеціальним підрозділам по боротьбі з організованою злочинністю Служби безпеки України та Міністерства внутрішніх справ України обласного рівня за місцезнаходженням банку.

Одна з вирішальних умов економічної безпеки – постійне вдосконалення законодавства, спрямованого на протидію легалізації «брудних» коштів. Запроваджується в життєву практику прийнятий Верховною Радою закон «Про запобігання та протидію легалізації («відмиванню») доходів, одержаних злочинним шляхом». Нарощують свої зусилля в цьому органи державної виконавчої влади й місцевого самоврядування, судово-правова система. У Генеральній прокуратурі України засновано Спеціальне управління з нагляду за розслідуванням кримінальних справ стовно «відмивання» «брудних» коштів.

«Відмивання» «брудних» коштів – це технології приховування сумнівного джерела фінансів і перетворення їх на легальні, дозволені. Спочатку в міжнародних домовленостях такими коштами вважали гроші, отримані від наркобізнесу. Але оскільки організована злочинність дедалі частіше почала вдаватися до багатьох інших видів злочинної діяльності та ще й поєднувати їх, то нині світова практика вважає «брудними» будь-які кошти, набуті злочинним, незаконним, аморальним шляхом. У цілому нині в цивілізованих країнах до джерел «брудних» грошей відносять не тільки наркотичні операції, а й тероризм, корупцію, шахрайство, шантаж.

Боротьба з легалізацією доходів, здобутих незаконним шляхом, – це один із чинників економічної безпеки України. Нині щонайсерйозніше занепокоєння викликають саме втрати, яких завдає «відмивання» грошей господарському комплексові. Воно тісно пов'язане з такими явищами, як відплив капіталу, використання для його приховування офшорів. Це одна з головних причин несприятливого інвестиційного клімату в Україні.

Боротьба з легалізацією «брудних» коштів необхідна, зокрема, щоб захистити вітчизняну фінансову систему від негативного впливу світового кримінального капіталу.

Формування української правової бази та управлінських органів з протидії «відмиванню» «брудних» коштів і тероризмові схвально сприймається

громадянами України. Це, власне, одна з основ її доброго імені в Європейському співтоваристві. Адже чорний список можна розцінювати по-різному. Карою тому, хто його заслужив або застереженням чи підказкою для того, хто оступився і виправляє помилку.

Лише останнім часом видано регуляторні акти, як, наприклад, липневий президентський указ 2001 р. «Про додаткові заходи щодо боротьби з «відмиванням доходів», одержаних злочинним шляхом». Для їх реалізації уряд ухвалив цілу низку конкретизуючих нормативних документів. Відповідний правовий акт прийнято четвертим скликанням ВР 28 листопада 2002 р. З його ухваленням було внесено зміни до закону «Про фінансові послуги і державне регулювання ринків фінансових послуг» та до КК України та Кодексу про адміністративні правопорушення.

17 січня 2001 р. набрав чинності Закон України «Про банки і банківську діяльність», до якого включена спеціальна глава 11 «Запобігання легалізації грошей, набутих злочинним шляхом». Однак окремі його Положення не позбавлені неузгодженості, зокрема із законодавством з питань боротьби з організованою злочинністю.

Так, ст.59 цього Закону передбачає, що арешт на майно або кошти банку, що є на його рахунках, а так само арешт на кошти та інші цінності юридичних або фізичних осіб, що містяться в банку, накладається виключно за санкціонованою прокурором Постановою слідчого, за Постановою державного виконавця у випадках, передбачених законами України або за рішенням суду.

Це Положення не узгоджується із Законом України «Про організаційно-правові основи боротьби з організованою злочинністю», пунктом 46 ст.12, якою спецпідрозділам надано право за постановою та із санкції відповідного прокурора накладати арешт на грошові кошти та інші цінності фізичних та юридичних осіб.

У зв'язку з цим виникає потреба у внесенні відповідних змін до п. 46 ст.12 України «Про організаційно-правові основи боротьби з організованою злочинністю», замінивши слова «... накладати арешт на грошові кошти та інші цінності фізичних та юридичних осіб...» на слова «... призупиняти рух грошових коштів у видатковій частині по рахунках юридичних та фізичних осіб у банках, накладати арешт на інші цінності юридичних та фізичних осіб».

Останнім часом ускладнився контроль за діяльністю банків. Це викликано тим, що Оболонський районний суд м.Києва 13 листопада 2001 р. прийняв рішення про визнання недійсною Постанову Правління НБУ від 17 липня 2001 р. № 276 «Про планування і порядок проведення інспекційних перевірок» у частині проведення Національним банком України таких видів перевірок, як вступний контроль, спеціальна

перевірка, тематична перевірка, а також прийняття Національним банком України рішення про проведення позапланових перевірок за наявності таких підстав, як звернення органів прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, Державної податкової служби України, Координаційного комітету боротьби з організованою злочинністю при Президентові України. Зазначене рішення Оболонського районного суду м. Києва вступило в дію 6 лютого 2002 р.

Тому Національний банк України, а також його регіональні відділення за цим рішенням не можуть провадити позапланові перевірки банків за запитами правоохоронних органів.

Відсутність законодавчо закріпленої норми, яка б регламентувала порядок проведення позапланових тематичних перевірок банків за зверненнями правоохоронних органів істотно ускладнює процес розкриття і документування правопорушень у банківській сфері, зокрема пов'язаних з легалізацією («відмиванням») коштів.

Але самими кримінально-правовими засобами досконалої системи протидії «відмиванню» не створиш. Сюди треба долучати ще й заходи у сферах адміністративного, фінансового законодавства. Лише така цілісність може стати правовим підґрунтям для виваженої та послідовної державної політики у цій галузі.

Створення ефективної системи заходів із запобігання і боротьби з легалізацією брудних коштів є завданням загальнодержавного рівня, реалізація якого дасть можливість своєчасно виявляти та припиняти злочинний бізнес, що продукує сумнівні доходи. Це трансформувалось у Законі «Про запобігання та протидію легалізації («відмиванню») доходів, одержаних злочинним шляхом».

Проте Україна й далі залишається в так званому «чорному списку» FATF, що негативно впливає на міжнародний імідж країни. Ціла низка питань залишилася ще не вирішеними. Зокрема не визначений порядок відмови в обслуговуванні клієнта, передбачений ст.64 Закону України «Про банки і банківську діяльність», у разі ненадання останнім необхідних документів або умисного подання неправдивих відомостей. Цей порядок повинен бути нормативно врегульованим і єдиним для всіх банків, що дасть змогу уникнути різних тлумачень норм закону, а також не допустити елементів недобросовісної конкуренції на банківському ринку.

Іншим спірним питанням є вимога НБУ щодо обов'язкового входження до правління банку відповідального працівника, який очолює внутрішньобанківську систему запобігання легалізації коштів, одержаних злочинним шляхом. Однак згідно з чинним законодавством призначення членів правління є прерогативою вищих органів управління банку – загальних зборів або спостережної ради.

Система запобігання використанню банків для відмивання коштів може бути ефективною тільки за умови участі в ній широкого кола банківських працівників, які безпосередньо обслуговують клієнтів.

Важливу роль у захисті БСУ відіграють заходи із запобігання використанню електронних і пластикових засобів у злочинних цілях, які будуть розглянуті у наступному підрозділі.

3.4. Основі засади побудови захисту банківських автоматизованих систем, електронних платежів та персональних платежів фізичних осіб

Під безпекою АСОІБ слід розуміти їх властивість, що виражається в здатності протидіяти спробам нанесення збитку власникам і користувачам системи при різних (навмисних і ненавмисних) діях. Тобто захищеність від випадкового чи навмисного втручання в процес функціонування цієї системи, а також від спроб розкрадання чи руйнування її компонентів. Безпека АСОІБ досягається забезпеченням конфіденційності оброблюваної нею інформації, а також цілісності й доступності компонентів і ресурсів системи.

Конфіденційність інформації АСОІБ – це властивість інформації бути відомою тільки допущеним і перевіреним суб'єктам системи (користувачам, програмам, процесам та ін.). Для інших суб'єктів системи ця інформація недоступна.

Цілісність компонента (ресурсу) системи – властивість компонента (ресурсу) бути незмінним (у семантичному змісті) при функціонуванні системи.

Доступність компонента (ресурсу) системи – властивість компонента (ресурсу) бути доступним для використанням авторизованими суб'єктами системи в будь-який час [192, с. 57].

Кінцевою метою вживання заходів протидії загрозам є захист власника і законних користувачів АСОІБ від нанесення їм матеріального чи морального збитку в результаті випадкових чи навмисних впливів на неї.

Розрізняють зовнішню і внутрішню безпеку АСОІБ [193, с. 182]. Зовнішня безпека включає захист АСОІБ від стихійних лих (пожежа, повінь тощо) і від проникнення зловмисників ззовні з метою розкрадання, отримання доступу до носіїв чи інформації, виводу системи з ладу. Предметом внутрішньої безпеки є забезпечення надійної роботи системи, цілісності її програм і даних. Усі зусилля із забезпечення внутрішньої безпеки АСОІБ фокусуються на створенні надійних та зручних механізмів регламентації діяльності всіх її користувачів і обслуговуючого персоналу,

дотриманні встановленої в організації дисципліни прямого чи непрямого доступу до ресурсів системи і до інформації.

Побудову системи інформаційної безпеки варто починати з аналізу ризиків можливих загроз. Ризик – це визначення вірогідності події, що веде до втрат. Для оцінки ступеня ризику при тому чи іншому варіанті дій застосовуються різні методики. У закордонній літературі вони отримали назву «аналіз ризику» (risk analysis). Аналіз ризику застосовується до всіляких операцій. Наприклад, при видачі кредиту фахівці банку оцінюють ризик його неповернення позичальником. Оцінивши величезний ступінь ризику можна вжити заходів, які спрямовані на його зменшення (наприклад, опечатавши на складі позичальника високоліквідний товар) [196, с. 28].

Перед тим, як вибирати різні засоби захисту слід чітко представляти які компоненти АСОІБ, від яких зазіхань і наскільки надійно ви хочете захистити. Безумовно, основою системи захисту АСОІБ мають бути організаційні (адміністративні) заходи, стрижнем яких є розробка і реалізація плану захисту.

Аналіз ризику – це процес отримання кількісної чи якісної оцінки збитку, що може виникнути у випадку реалізації загроз безпеці АСОІБ.

Нижче розглядаються основні етапи проведення аналізу ризику безпеки АСОІБ. Вони можуть в окремих випадках корегуватися залежно від конкретних умов аналізу [196, с. 29]: опис компонентів АСОІБ; визначення уразливих місць АСОІБ; оцінка імовірностей прояву загроз безпеці АСОІБ; оцінка очікуваних розмірів втрат; огляд можливих методів захисту й оцінка їхньої вартості; оцінка вигоди від вживання передбачуваних заходів.

Розглянемо ці етапи докладніше.

Опис компонентів АСОІБ

Компоненти АСОІБ – це :

– устаткування – ЕОМ і їхні складові (процесори, монітори, термінали, робочі станції), периферійні пристрої (дисководи, пристрої back-up, порти виводу-вводу-висновку, принтери, кабелі, контролери, лінії зв'язку) і т.ін.;

– програмне забезпечення – вихідні, об'єктні, завантажувальні модулі, придбані програми, «домашні» розробки, утиліти, операційні системи і системні програми (компілятори, компоновщики й ін.), діагностичні програми тощо;

– дані – тимчасові, збережені постійно, на магнітних носіях, друковані, архівні, системні журнали і т.ін.;

– співробітники – користувачі й обслуговуючий персонал.

Захист від прояву тієї чи іншої загрози може бути реалізований різними засобами. Наприклад, захистити інформацію на твердому диску ПЕОМ можна такими засобами: організувати контроль за доступом у приміщення, в якому встановлена ПЕОМ; призначити відповідальних за використання ПЕОМ; шифрувати інформацію на диску; використовувати системи розмежування доступу; закривати доступ чи демонтувати дисководи і порти виводу-вводу-висновку; застосовувати засоби оповіщення адміністратора про розкриття корпуса ПЕОМ.

Специфічною рисою електронних банківських систем є спеціальна форма обміну електронними даними, без яких жоден сучасний банк не може існувати. Обмін електронними даними (ОЕД) – це міжкомп'ютерний обмін діловими, комерційними, фінансовими електронними документами.

ОЕД забезпечує оперативну взаємодію торгових партнерів (клієнтів, постачальників, торгових посередників і ін.) на всіх етапах підготовки торгової угоди, укладання контракту і реалізації постачання. На етапі оплати контракту і переказу коштів ОЕД може забезпечувати електронний обмін фінансовими документами. При цьому створюється ефективне середовище для торгово-платіжних операцій [193, с. 71].

ОЕД використовується як перевага в конкурентній боротьбі, що дозволяє більш тісно взаємодіяти з партнерами. Така стратегія прийнята у великих організаціях і одержала назву «Підходу Розширеного Підприємства» (Extended Enterprise) [186, с. 230].

Основною перешкодою ОЕД є значне різноманіття документів, якими обмінюються через канали зв'язку. Для подолання цієї перешкоди були розроблені стандарти представлення документів у системах ОЕД для різних галузей діяльності [186, с. 234].

Складовою ОЕД є електронні платежі – обмін фінансовими документами між клієнтами і банками, між банками й іншими фінансовими і комерційними організаціями. Суть концепції електронних платежів полягає в тому, що повідомлення, які пересилаються лініями зв'язку, належним чином оформлені та передані, і є підставою для виконання однієї чи кількох банківських операцій. Ніяких документів на папері для виконання цих операцій не потрібно (хоча вони можуть бути видані). Іншими словами повідомлення, яке пересилається лініями зв'язку, несе інформацію про те, що відправник виконав деякі операції над своїм рахунком, зокрема над кореспондентським рахунком банку-одержувача (у ролі якого може виступати кліринговий центр), і що одержувач повинен виконати зазначені в повідомленні операції. За допомогою такого повідомлення можна переслати чи одержати гроші, відкрити кредит, оплатити покупку чи послугу і виконати будь-яку іншу банківську

операцію. Такі повідомлення називаються електронними грошима, а виконання банківських операцій на підставі відправлення чи отримання таких повідомлень – електронними платежами. Природно, весь процес проведення електронних платежів має потребу в надійному захисті. Інакше банк і його клієнтів очікують серйозні неприємності.

Міжбанківські й торгові розрахунки провадяться між організаціями (юридичними особами), тому їх іноді називають корпоративними. Розрахунки за участю фізичних осіб-клієнтів одержали назву персональних.

Більшість великих розкрадань у банківських системах прямо чи побічно пов'язано саме з електронними платежами.

На шляху створення систем електронних платежів, особливо глобальних, що охоплюють велике число фінансових інститутів і їхніх клієнтів у різних країнах, зустрічається безліч перешкод. Основними з них є:

– відсутність єдиних стандартів на операції та послуги, що істотно ускладнює створення об'єднаних банківських систем. Кожен великий банк прагне створити свою мережу ОЕД, а це збільшує витрати на її експлуатацію і зміст;

– зростання мобільності грошових мас, що веде до збільшення можливості фінансових спекуляцій, розширює потоки «блукаючих капіталів». Ці гроші здатні за короткий час змінювати ситуацію на ринку, дестабілізувати її;

– збої та відмовлення технічних і помилки програмних засобів при проведенні фінансових розрахунків, що може призвести до серйозних ускладнень для подальших розрахунків і втрати довіри до банку з боку клієнтів, особливо внаслідок тісного переплетення банківських зв'язків. При цьому істотно зростає роль та відповідальність операторів і адміністрації системи, які безпосередньо керують обробкою інформації.

Для надійної роботи система електронних платежів повинна бути добре захищена. Торгові розрахунки виробляються між різними торговими організаціями. Банки в цих розрахунках беруть участь як посередники у разі перерахування грошей з рахунка організації-платника на рахунок організації-одержувача. Такі розрахунки надзвичайно важливі для загального успіху програми електронних платежів. Обсяг фінансових операцій різних компаній зазвичай складає значну частину загального обсягу операцій банку.

Види торгових розрахунків істотно вирізняються між собою для різних організацій, але завжди при їх проведенні обробляється два типи інформації: платіжні повідомлення і допоміжна (статистка, зведення, повідомлення). Для фінансових організацій найбільший інтерес становить зазвичай інформація платіжних повідомлень – номери рахунків, суми,

баланс і т.ін. Для торгових організацій обидва види зведень однаково важливі – перший дає ключ до фінансового стану, другий допомагає при прийнятті рішень і виробленні політики.

Кожну систему обробки інформації захисту варто розробляти індивідуально з огляду на такі особливості: організаційну структуру банку; обіг і характер інформаційних потоків (усередині банку в цілому, усередині відділів, між відділами, зовнішніх); кількість і характер клієнтів; графік добового навантаження.

Побудова захисту АСОІБ має також враховувати як загальні правила, так і зазначені нижче етапи:

– аналіз ризику, що закінчується розробкою проекту системи захисту і планів захисту, безупинної роботи і відновлення; реалізація системи захисту на основі результатів аналізу ризику;

– постійний контроль за роботою системи захисту й АСОІБ у цілому (програмний, системний і адміністративний).

На кожному етапі реалізуються певні вимоги до захисту; їхнє точне дотримання приводить до створення безпечної системи.

На сьогодні захист АСОІБ – це самостійний напрямок досліджень. Для забезпечення безупинного захисту інформації в АСОІБ доцільно створити з фахівців групу інформаційної безпеки.

Основні етапи побудови системи захисту такі: аналіз, розробка системи захисту (планування); її реалізація; супровід.

На стадії планування формується система захисту як єдина сукупність заходів протидії.

За способами вживання всі заходи забезпечення безпеки комп'ютерних систем поділяються на: правові, морально-етичні, адміністративні, фізичні і технічні (апаратні й програмні) [200, С.28].

До правових заходів захисту відносяться чинні закони, укази, постанови й інші нормативні акти, що регламентують правила роботи з інформацією обмеженого використання і відповідальність за їх порушення. Вони перешкоджають несанкціонованому використанню інформації та є стимулюючим чинником для потенційних порушників.

До морально-етичних заходів протидії відносяться всілякі норми поведінки, що традиційно складаються в міру поширення ЕОМ у БСУ. Ці норми здебільшого не є обов'язковими як законодавчо затверджені, однак їхнє недотримання веде, зазвичай, до падіння авторитету, престижу людини чи групи осіб. Морально-етичні норми бувають як неписані (наприклад, загальновизнані норми честі, патріотизму тощо), так і оформлені в кодекс чи правила. Найхарактернішим прикладом останніх є «Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США» [203]. Зокрема, вважаються неетичними навмисні чи ненавмисні дії, що викликають додаткові

невиправдані витрати ресурсів (машинного часу, пам'яті, каналів зв'язку тощо); порушують цілісність збереженої й оброблюваної інформації; зачіпають інтереси інших законних користувачів і т.ін.

Адміністративні заходи захисту – це заходи організаційного характеру, що регламентують процеси функціонування системи обробки інформації, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити чи унеможливити реалізацію загроз безпеці. Вони включають: розробку правил обробки інформації в АСОІБ; заходи, вживані при проектуванні, будівництві й устаткуванні обчислювальних центрів та інших об'єктів АСОІБ (урахування впливу стихії, пожеж, охорона приміщень, організація захисту від установки апаратури, що прослухує, і т.ін.); заходи, вживані при підборі й підготовці персоналу (перевірка нових співробітників; ознайомлення їх з порядком роботи з конфіденційною інформацією, з мірами відповідальності за порушення правил її обробки; створення умов, за яких персоналу було б невигідно припускатися зловживань і т.ін.); організацію обліку, збереження, використання та знищення документів і носіїв з конфіденційною інформацією.

Фізичні заходи захисту – це різного роду механічні, електро- чи електронні пристрої та обладнання, спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів системи й інформації, що захищається, організація надійного пропускного режиму.

Технічними засобами захисту є різні електронні пристрої і спеціальні програми, що виконують (самостійно чи в комплексі з іншими засобами) функції захисту (ідентифікацію й аутентифікацію користувачів, розмежування доступу до ресурсів, реєстрацію подій, криптографічний захист інформації тощо).

Найкращі результати досягаються за системного підходу до питань забезпечення безпеки АСОІБ і комплексного використання різних заходів захисту на всіх етапах життєвого циклу системи, починаючи із самих ранніх стадій її проектування.

У цій сфері важливо відпрацювати управління засобами захисту і відновлення та політику безпеки. Надійне управління здійсненне лише у випадку розуміння обслуговуючим персоналом розмірів можливих збитків, чіткого викладу планів і виконання персоналом своїх обов'язків. Багато співробітників, що обслуговують АСОІБ, не завжди усвідомлюють ризик, пов'язаний з обробкою інформації в АСОІБ. Тільки спеціальна попередня підготовка персоналу сприяє правильній та ефективній роботі засобів захисту й відновлення. Опис різних способів подолання і порушення захисту в повсякденній діяльності в сфері бізнесу (як, наприклад, витік

інформації до конкурента) допоможе обслуговуючому персоналу зрозуміти потребу точного виконання вимог захисту (наприклад, своєчасної зміни паролів).

Політика безпеки – це набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях.

Політика безпеки являє собою деякий набір вимог, що пройшли відповідну перевірку, реалізованих за допомогою організаційних і програмно-технічних засобів, що визначають структуру системи захисту. Її реалізація для конкретної АСОІБ провадиться за допомогою засобів управління механізмами захисту. Для конкретної організації політика безпеки має бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації тощо.

Основу політики безпеки складає спосіб управління доступом, який визначає порядок доступу суб'єктів системи до об'єктів системи.

На сьогодні найкраще вивчені два види політики безпеки: виборча і повноважна, засновані відповідно до виборчого і повноважного способу управління доступом.

Для того, щоб коректно втілити в життя розроблену політику безпеки слід мати надійні механізми її реалізації. Природно припустити, що всі засоби, які відповідають за реалізацію політики безпеки, самі повинні бути захищені від будь-якого втручання в їхню роботу. В іншому разі говорити про надійність захисту буде важко. Можна змінювати їхні параметри, але у своїй основі вони мають залишатися в недоторканності.

Тому всі засоби захисту і управління мають бути об'єднані в так звану достовірну обчислювальну базу.

Достовірна обчислювальна база (ДОБ) – це абстрактне поняття, що позначає цілком захищений механізм обчислювальної системи (включаючи апаратні та програмні засоби), відповідальний за підтримку реалізації політики безпеки.

ДОБ виконує подвійне завдання – підтримує реалізацію політики безпеки і є гарантом цілісності механізмів захисту, тобто самої себе. ДОБ спільно використовується всіма користувачами АСОІБ, однак її модифікація дозволена тільки користувачам зі спеціальними повноваженнями. До них належать адміністратори системи й інші співробітники банку. Процес, який функціонує від імені ДОБ, є достовірним. Це означає, що система захисту беззастережно довіряє цьому процесу і всі його дії санкціоновані політикою безпеки. Саме тому завдання номер один для захисту ДОБ – підтримка власної цілісності; усі програми і набори цих

ДОБ повинні бути надійно захищені від несанкціонованих змін. Для підтримки політики безпеки і власного захисту ДОБ маж забезпечити захист суб'єктів (процесів) та об'єктів системи в оперативній пам'яті і на зовнішніх носіях.

У моделі Белла-Лападулла (виборчої й повноважної політики безпеки) монітор посилань повинен контролювати стан системи і переходи з одного до іншого. Основними функціями, які має виконувати ядро безпеки разом з іншими службами ОС, є [186, с.193]:

1. Ідентифікація, аутентифікація й авторизація суб'єктів і об'єктів системи.

Ці функції потрібні для підтвердження дійсності суб'єкта, законності його прав на певний об'єкт чи на визначені дії, а також для забезпечення роботи суб'єкта в системі.

Ідентифікація – процес розпізнавання елементів системи за допомогою заздалегідь визначеного ідентифікатора чи іншої апріорної інформації; кожен суб'єкт чи об'єкт має бути однозначно ідентифікованим.

Аутентифікація – перевірка ідентифікації користувача, процесу чи пристрою, іншого компонента системи (зазвичай провадиться перед дозволом до доступу); а також перевірка цілісності даних при збереженні чи передачі для запобігання несанкціонованої модифікації.

Авторизація – надання суб'єкту прав на доступ до об'єкта.

Ці функції потрібні для підтримки дозвільного порядку доступу до системи і дотримання політики безпеки: авторизований (дозволений) доступ має тільки той суб'єкт, чий ідентифікатор відповідає результатам аутентифікації. Вони виконуються як у процесі роботи (при зверненні до наборів даних, пристроїв, ресурсів), так і при вході в систему.

2. Контроль входу користувача в систему і управління паролями. Ці функції є часткою зазначених вище: при вході в систему і введенні імені користувача провадиться ідентифікація, при введені пароля – аутентифікація і якщо користувач з таким іменем та паролем зареєстрований у системі, йому дозволяється доступ до визначених об'єктів і ресурсів (авторизація). Як показує практика, вхід користувача в систему – одне з найуразливіших місць захисту; відомі безліч випадків злому пароля, входу без пароля, перехоплення пароля і т.ін. Тому при виконанні входа, і користувач, і система повинні бути упевнені, що вони працюють безпосередньо один з одним, між ними немає інших програм, а інформація, що вводиться, достовірна.

Достовірний маршрут реалізується привілейованими процедурами ядра безпеки, чия робота забезпечується механізмами ДОБ, а також деякими іншими механізмами, що виконують допоміжні функції. Вони

перевіряють, наприклад, що термінал, з якого виконується вхід у систему, не зайнятий ніяким іншим користувачем, який імітував закінчення роботи.

3. Реєстрація і протоколювання. Аудит. Ці функції забезпечують отримання й аналіз інформації про стан ресурсів системи за допомогою спеціальних засобів контролю, а також реєстрацію дій, визнаних адміністрацією потенційно небезпечними для безпеки системи.

Більшість систем захисту мають у своєму розпорядженні засоби управління системним журналом. Системний журнал є складовою монітора посилань і слугує для контролю дотримання політики безпеки. Він є одним з основних засобів контролю, що допомагає адміністратору запобігати можливим порушенням.

Зміст системного журналу й інших наборів даних, що зберігають інформацію про результати контролю, повинні піддаватися періодичному перегляду й аналізу (аудиту) з метою перевірки дотримання політики безпеки.

4. Протидія «збору сміття». Після закінчення роботи програми оброблювана інформація не завжди цілком видаляється з пам'яті. Частина даних може залишатися в оперативній пам'яті, на дисках і стрічках, інших носіях. Вони зберігаються на диску до перезапису чи знищення. При виконанні цих дій на просторі диска, що звільняється, знаходяться їхні залишки.

Хоча при перекручуванні заголовка файлу ці залишки прочитати важко, однак з використанням спеціальних програм й устаткування така можливість все-таки є. Цей процес називається «збиранням сміття». Він може призвести до витоку важливої інформації.

5. Контроль цілісності суб'єктів. Відповідно до моделі Белла-Лападулла [186, С.196] безліч суб'єктів системи є підмножиною безлічі об'єктів, тобто кожен суб'єкт одночасно є об'єктом. При цьому під суб'єктом зазвичай розуміють зміст контексту процесу, куди входить зміст загальних і спеціальних регістрів (контекст процесу постійно змінюється). Крім змісту чи значення суб'єкт має низку специфічних атрибутів: пріоритет, список привілеїв, набір ідентифікаторів й інші характеристики. У цьому значенні підтримку цілісності суб'єкта, тобто запобігання його несанкціонованій модифікації, можна розглядати як окремий випадок такого завдання для об'єктів взагалі.

Контроль цілісності забезпечується процедурами ядра безпеки, контрольованими механізмами підтримки ДОБ. Основну роль грають такі механізми, як підтримка віртуальної пам'яті (для створення сфери зазначеного процесу) і режим виконання процесу (визначає його можливості в межах конкретної сфери і поза нею).

6. Контроль доступу. Під контролем доступу розуміють обмеження можливостей використання ресурсів системи програмами, процесами чи іншими системами (для мережі) відповідно до політики безпеки.

Основним об'єктом уваги засобів контролю доступу є спільно використовувані набори даних і ресурси системи. Спільне використання об'єктів породжує ситуацію «взаємної недовіри», за якої різні користувачі одного об'єкта не можуть до кінця довіряти один одному. І якщо з цим об'єктом будь-що трапиться, усі вони попадають у коло підозрюваних.

У чистому вигляді розглянуті принципи реалізації політики безпеки застосовуються рідко. Зазвичай використовуються їхні різні комбінації. Може відбутися витік інформації без порушення захисту, якщо погано була спроектована чи реалізована політика безпеки. Політика безпеки і механізми підтримки її реалізації утворюють єдине захищене середовище обробки інформації.

Існують два підходи до забезпечення безпеки АСОІБ – фрагментарний і комплексний.

«Фрагментарний» підхід орієнтується на протидію суворо визначених загроз за певних умов. Прикладами реалізації такого підходу є, наприклад, спеціалізовані антивірусні засоби, окремі засоби реєстрації і управління, автономні засоби шифрування і т.ін. Головна відмінна риса «фрагментарного» підходу – відсутність єдиного захищеного середовища обробки інформації. Головним достоїнством «фрагментарного» підходу є його висока вибірковість щодо конкретної загрози, що зумовлює і основний його недолік – локальність дії.

Особливістю комплексного підходу є створення захищеного середовища обробки інформації в АСОІБ, що поєднує різні заходи протидії загрозам (правові, організаційні, програмно-технічні). Захищене середовище обробки інформації будується на основі розроблених для конкретної АСОІБ правил обробки критичної інформації. Організація захищеного середовища обробки інформації дозволяє гарантувати (у межах розробленої політики безпеки) рівень безпеки АСОІБ. Недоліками підходу є висока чутливість до помилок установки і настроювання засобів захисту, складність управління, обмеження свободи дій користувачів АСОІБ.

Комплексного підходу дотримуються більшість державних і великих комерційних підприємств та установ, він знайшов своє відображення у різних стандартах і цілеспрямовано вводиться в життя, наприклад, Міністерством оборони США в особі Національного Центру Комп'ютерної Безпеки (NCSC) [186, с. 201].

Основу повноважної політики безпеки складає повноважне управління доступом, мається на увазі, що: усі суб'єкти й об'єкти системи повинні бути однозначно ідентифіковані; кожному об'єкту системи присвоєна влучна критичність, яка визначає цінність інформації, що міститься в ньому; кожному

суб'єкту системи присвоєний рівень прозорості, який визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Кожен суб'єкт крім рівня прозорості має поточне значення рівня безпеки, що може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Для моделювання повного управління доступом використовується модель Белла-Лападула [186, с. 159], що містить поняття безпечного (з погляду політики) стану і переходу. Для ухвалення рішення на дозвіл доступу виробляється порівняння мітки критичності об'єкта з рівнем прозорості і поточним рівнем безпеки суб'єкта. Результат порівняння визначається двома правилами: «простою умовою захисту» і «властивістю». У спрощеному вигляді вони визначають, що інформація може передаватися тільки «наверх», тобто суб'єкт може читати вміст об'єкта, якщо його поточний рівень безпеки не нижче критичності об'єкта, і записувати в нього, – якщо не вище.

Основне призначення повноважної політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності та запобігання витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливих проникнень з нижніх рівнів на верхні. При цьому вона функціонує на тлі виборчої політики, надаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Крім управління доступом суб'єктів до об'єктів системи проблема захисту інформації має ще один аспект. Щоб отримати інформацію про будь-який об'єкт системи, зовсім не обов'язково шукати шляхи несанкціонованого доступу до нього. Можна отримувати інформацію спостерігаючи за роботою системи і, зокрема за обробкою потрібного об'єкта. Іншими словами, за допомогою каналів витоку інформації. За цими каналами можна отримати інформацію не тільки про вміст об'єкта, але й про його стан, атрибути тощо залежно від особливостей системи і встановленого захисту об'єктів. Ця особливість пов'язана з тим, що у разі взаємодії двох суб'єктів виникає деякий потік інформації від одного до іншого.

Інформаційні потоки існують у системі завжди. Тому виникає потреба у визначенні, які з інформаційних потоків в системі є «легальними», тобто не ведуть до витоку інформації, а які – ні. Таким чином, виникає потреба у розробці правил, що регулюють управління інформаційними потоками в системі.

Для цього слід побудувати модель системи, що може описувати такі потоки. Така модель називається потоковою [186, С.176]. Модель описує умови і властивості взаємного впливу (інтерференції) суб'єктів, а також кількість інформації, отриманої суб'єктом у результаті інтерференції.

Управління інформаційними потоками застосовується, зазвичай, в межах вибіркової чи повноважної політики, доповнюючи їх і підвищуючи надійність системи захисту.

Управління доступом (вибіркове чи повноважне) є порівняно легко реалізованим (чи апаратно програмним), однак воно неадекватне реальним АСОІБ через існування в них прихованих каналів. Проте управління доступом забезпечує досить надійний захист у простих системах, що не обробляють особливо важливу інформацію. В іншому випадку засоби захисту повинні додатково реалізовувати управління інформаційними потоками. Організація такого управління в повному обсязі достатньо складна, тому його, як правило, використовують для посилення надійності повноважної політики: неспадні (щодо рівнів безпеки) інформаційні потоки вважаються дозволеними, всі інші – забороненими.

Відзначимо, що крім способу управління доступом політика безпеки включає ще й інші вимоги, такі як підзвітність, гарантії тощо.

Вибіркове і повноважне управління доступом, а також управління інформаційними потоками – свого роду три кити, на яких будується весь захист.

З погляду захисту в системах ОЕД існують такі вразливі місця: пересилання платіжних та інших повідомлень між банками чи між банком і клієнтом; обробка інформації усередині організацій відправника й одержувача; доступ клієнта до засобів, акумульованих на рахунку.

Одне з найуразливіших місць у системі ОЕД – пересилання платіжних й інших повідомлень між банками, чи між банком і банкоматом, чи між банком та клієнтом.

З технічного погляду ці проблеми визначаються за допомогою кількох механізмів, що відповідають за забезпечення адекватної безпеки електронних банківських систем. Робота більшості цих механізмів забезпечується службами мережі з розширеним набором послуг (Value-Added Network, VAN). Служби, що реалізують ОЕД, мають виконувати такі функції:

– забезпечувати захист від випадкових і навмисних помилок;

– забезпечувати адаптацію до частих змін кількості користувачів, типів устаткування, способів доступу, обсягів трафіка, топології;

– підтримувати різні типи апаратного і програмного забезпечення, що поставляється різними виробниками;

– здійснювати управління та підтримку мережі для забезпечення безперервності роботи і швидкої діагностики порушень;

– реалізовувати повний спектр прикладних завдань ОЕД, включаючи електронну пошту;

– реалізовувати максимально можливу кількість вимог партнерів;

– включати служби резервного копіювання і відновлення після аварій.

Повнота вирішення розглянутих вище проблем залежить від правильного вибору системи шифрування. Система шифрування (чи криптосистема) являє собою сукупність алгоритмів шифрування і методів поширення ключів.

Слід зазначити, що у разі захисту систем ОЕД велику роль відіграє не стільки шифрування документа, скільки забезпечення його цілісності й аудентифікація абонентів (джерела даних) при проведенні сеансу зв'язку. Тому механізми шифрування в таких системах відіграють звичайно допоміжну роль.

Надійність усієї криптосистеми в цілому багато в чому залежить від механізмів розподілу ключів між учасниками взаємодії. У кожному конкретному випадку вона повинна визначатися з урахуванням особливостей функціонування всієї АСОІБ. Існує багато різних підходів до розв'язання цієї проблеми. Ми не розглядаємо детально кожен із них, оскільки це виходить далеко за межі мети нашого дослідження і вони детально охарактеризовані [186, С.305].

Потреба у підтримці електронних банківських послуг за допомогою спеціальних банківських та інших мереж, а також за допомогою національних клірингових систем радикально змінила відносини між банками і їхніми клієнтами. Тільки за останнє десятиліття стали доступними, та використовуються повсюдно різні клірингові системи, що виконують весь спектр банківських операцій. Дані й інструкції вводяться, розподіляються та обробляються в них у режимі реального часу.

Безпека операцій з готівкою і розрахунковими послугами вимагає вжиття тих самих загальних заходів, які потрібні для захисту будь-якої електронної фінансової послуги. Особливу увагу слід звернути на захист терміналів, підключених до систем електронних платежів.

Якщо банк виконує операції підвищеного ризику, то реалізовані процедури забезпечення безпеки повинні включати парольний захист, багаторівневу авторизацію користувачів, контроль операцій, ведення системного журналу. Також варто розмежовувати доступ користувачів до терміналів і інших зовнішніх пристроїв, що мають бути захищені фізично. Для забезпечення безпеки даних, переданих по лініях зв'язку, слід використовувати криптографічні методи.

Система безпеки центральної АСОІБ слід включати багаторівневий контроль доступу до периферійних пристроїв і центральної бази даних.

Якщо операції підвищеного ризику не виконуються, деякі вимоги до безпеки можуть бути ослаблені чи ліквідовані зовсім. Завдання щодо забезпечення безпеки визначаються для кожного конкретного випадку індивідуально в процесі аналізу ризику.

Сьогодні у світі існує велика кількість систем електронних платежів. Найвідоміші з них [186, с. 312]:

– S.W.I.F.T. (The Society for Worldwide Inter-bank Financial Telecommunication) – безприбуткове кооперативне міжнародне співтовариство, метою якого є організація міжбанківських розрахунків в усьому світі.

– FedWire – сама велика система американських міжбанківських комунікацій, що з'єднує головні контори округу Federal Reserve, галузі банків Federal Reserve і більше 500 інших банків за допомогою центра комутації у Вірджинії.

– CHAPS (Clearing Houses Automated Payment System) – система підтримки електронних платежів між порівняно невеликою (близько 300) групою банків Лондона, більшість з який відділення іноземних банків, що використовують Лондон як розрахунковий центр.

– CHIPS (Clearing Houses Interbank Payment System) – клірингова система США, організована Нью-йоркською асоціацією клірингових палат (New York Clearing House Association – NYCHA) [195].

Виділяють чотири види персональних платежів: домашнє (телефонне) обслуговування; розрахунок через автоматичний касовий апарат (банкомат); розрахунок у точці продажу; фінансовий сервіс з використанням всесвітньої мережі Інтернет.

При обслуговуванні персональних платежів фізичних осіб широко використовуються пластикові картки. На сьогодні випущено більше мільярда карток у різних країнах світу [197, с. 26]. Найпоширеніші з них: кредитні картки Visa (більш 350 млн карток) і MasterCard (200 млн карток); міжнародні чекові гарантії Eurocheque і Posteheque; картки для оплати подорожей і розваг American Express (60 млн карток) і Diners Club.

За принципом дії можна виділити пасивні й активні пластикові картки. Пасивні усього лише зберігають інформацію на тому чи іншому носії. Відмінною рисою активних карток є наявність вмонтованої в них мікросхеми. Картка з мікропроцесором називається «інтелектуальною» (smart card).

За характером розрахунків, проведених з використанням пластикових карток, можна виділити кредитні і дебетові картки.

За характером використання картки підрозділяються на корпоративні й особисті. Головна відмінність корпоративних (які можуть бути видані тільки юридичним особам) від індивідуальних полягає в тому, що їхні власники мають право на отримання додаткових послуг.

На магнітній картці розміщена магнітна смуга, що складається з трьох доріжок. Кожна з них має відповідне призначення. Розміри картки, формат збережених даних визначені спеціальним стандартом ISO 7811 1985 р.

Процесорний тип карток винайдений і запатентований Роланом Мореном у Франції. Мікросхеми, встановлені на картці, можуть бути як звичайними – енергонезалежної пам'яті, так і досить складними мікропроцесорами. Ємність звичайної картки з енергонезалежною пам'яттю складає від 2 до 16 кілобайт. У постійно запам'ятовуючий пристрій, установлений на картці, прошивається спеціальний набір програм. Серцем таких карток є не просто мікропроцесор, а мікроЕОМ. Ці картки забезпечують великий набір функцій: можливість роботи із захищеною файловою системою; шифрування даних із застосуванням різних алгоритмів; ведення ключової системи і т.ін.

Деякі картки забезпечують режим «самоблокування» (неможливість подальшої роботи з нею) при спробі несанкціонованого доступу.

Перевагою інтелектуальних карток є більший обсяг збереженої інформації, стійкість до підробки і можливість використання в багатьох додатках.

Водночас інтелектуальні картки мають також істотні недоліки, які зумовили їхнє обмежене поширення. Основних недоліків два: висока вартість виробництва картки; збільшена порівняно із стандартом товщина. Для читання таких карток потрібна установка спеціальних зчитувачів.

Кредитні картки – найбільш розповсюджений тип пластикових карток. До них відносяться картки загальнонаціональних систем США Visa і Mastercard, American Express і Amex's Optima, Discovery Card фірми Sears Universal Card фірми AT&T, місцеві і регіональні картки універсальних магазинів.

Картки пред'являються на підприємствах торгівлі й обслуговування для оплати товарів і послуг. При оплаті за допомогою кредитних карток банк покупця відкриває йому кредит на суму покупки і потім через якийсь час (зазвичай 25 днів) надсилає рахунок поштою. Покупець повертає оплачений чек назад у банк.

Visa, MasterCard і Discover вимагають від власників карток принаймні фіксованого мінімального платежу.

Різновидом кредитних карток є affinity-картки. Вони випускаються банком, кредитним чи об'єднаним, фінансовою компанією, що уклали спеціальну угоду з професійною, суспільною, релігійною чи іншою некомерційною організацією. Зазвичай знак цієї організації міститься на кредитній картці. Виробник карток зобов'язується відчисляти своєму контрагенту якийсь (порівняно невеликий) відсоток від прибутку у разі використання карток. У відповідь на це організація, з якою укладений договір, допомагає виробнику карток впровадити їх серед її членів.

Дебетові картки використовуються для дебетових розрахунків. Інші її назви: картка наявних засобів чи розрахункова. Вона багато в чому

аналогічна кредитній. Дебетові картки призначені для заміни готівки і персональних чеків.

Пластикова картка, як основний носій інформації, є привабливим об'єктом для зловмисника. Тому перед випуском таких карток слід чітко уявляти ступінь їхнього захисту від різних впливів. Існує дві основні вимоги до банківських карток: унікальність і необоротність.

Перша вимога означає, що серед усіх випущених банком карток не повинно бути двох однакових за характеристиками. Створення подібної картки має бути виключене для зловмисника. Відповідно до другої вимоги – не може бути відновлена первісна інформація на картці.

Для реалізації цих вимог кожна фірма-виробник передбачає свої схеми захисту, всі тонкості яких вона зберігає в секреті. Розглянемо два основних способи захисту магнітних карток від підробки: метод магнітних водяних знаків і метод «сандвіча».

Метод магнітних водяних знаків передбачає нанесення на магнітну стрічку, розташовану на картці, спеціального малюнка. Цей малюнок наноситься за допомогою магнітного поля і виконує ту саму саму функцію, що і звичайні знаки на цінних паперах. При виготовленні картка піддається впливу сильного електромагнітного поля під кутом 45^0 до вздовжньої осі. Потім на неї впливає спеціальний записуючий пристрій, що перетворить направленість магнітних полів на картці до особливого виду.

Метод «сандвіча» є альтернативою методу водяних знаків і полягає в тому, що одна смужка містить ділянки з різними рівнями намагніченості, причому ділянка з меншою намагніченістю розташована ближче до голівки читання/запису. Для запису інформації на картку використовується сильне магнітне поле. У зчитувачів інформації картка спочатку проходить через поле, що стирає. При цьому на ділянці зі слабкою намагніченістю інформація стирається, а із сильною намагніченістю – не змінюється. Потім інформація зі смуги зчитується звичайним чином. Надійність цього способу захисту заснована на двох припущеннях: по-перше, якщо зловмисник використовує одинарну смугу для підробки картки, то вся інформація на ній буде затерта полем, що стирає; по-друге, для запису на двошарову смугу потрібно спеціальне устаткування для створення потрібного за величиною магнітного поля.

Сучасні пластикові картки мають кілька ступенів (рівнів) захисту. Наприклад, картки системи VISA мають сім рівнів захисту. На сьогодні не існує достовірної статистики стосовно втрат, що пов'язані з використанням пластикових карток. За деякими оцінками, вони складають до $ 2 млрд у рік. Основною причиною втрат є неправильне використання карток їхніми законними власниками [202].

Пропорції зловживань із пластиковими картками залежать від структури банківської індустрії і тому сильно змінюються від країни до країни. Наприклад, порівняно із Західною Європою, у США великі втрати відбуваються саме за рахунок неправильного використання карток. Але при цьому за оцінками експертів, збиток від шахрайства із застосуванням технічних засобів складає не менше $ 500 млн у рік [193, с. 52].

Нижче наведена статистика втрат для Visa і MasterCard (дані 1993 р.) [186, с. 24].

Таблиця 6

Причина	Частка в загальних збитках, %
Шахрайство продавця	22.6
Украдені картки	17.2
Підробка карток	14.3
Зміна рельєфу картки	8.1
Загублені картки	7.5
Неправильне застосування	7.4
Шахрайство по телефону	6.3
Шахрайство при пересиланні поштою	4.5
Поштове шахрайство	3.6
Крадіжки при виробництві, пересиланні	2.9
Змова із власником картки	2.1
Інші	3.5

Одна з найважливіших вимог безпеки при роботі з пластиковими картками – забезпечення безпеки банкоматів.

Сьогодні на автоматичні касові апарати (БАК) покладаються такі завдання:

– ідентифікація й аутентифікація клієнта;
– видача готівки;
– оповіщення про стан рахунка клієнта;
– переказ грошей клієнта з одного рахунка на інший;
– реєстрація всіх зроблених операцій і видача квитанцій.

Основне завдання БАК – видача готівки клієнту. Усередині БАК крім різних пристроїв знаходиться і готівка, отже повинно бути передбачено його серйозний фізичний захист.

За наявними даними [192, С.82] у Великій Британії БАК встановлені:

– 67% – вмонтовані в стіну;
– 21% – усередині банків;
– 5% – у вестибулях банків;
– 7% – окремо стоять банкомати поза банками.

При розгляді подальшого захисту збереженої в БАК інформації передбачається, що порушення його зовнішнього фізичного захисту малоймовірно.

Автоматичний касовий апарат може працювати в одному з двох режимів:

1. Off-line (автономний режим). В автономному режимі БАК функціонує незалежно від комп'ютерів банку. При цьому запис інформації про трансакції робиться на внутрішній магнітний диск і виводиться на вбудований принтер.

2. On-line (режим реального часу). Для роботи в цьому режимі БАК повинен бути приєднаний (безпосередньо або через телефонну мережу) до головного комп'ютера банку. При цьому реєстрація трансакцій провадиться безпосередньо на головному комп'ютері, хоча підтвердження про трансакції видається на принтер БАК.

Як автономний режим роботи БАК, так і режим реального часу мають свої переваги і недоліки.

Перевагами автономного режиму БАК є його відносна дешевизна і незалежність від якості ліній зв'язку. Особливо за вітчизняних умов, коли якість телефонних ліній, м'яко кажучи, не ідеальна. Водночас низька вартість установки зумовлює високу вартість експлуатації цих апаратів. Адже для того, щоб поновляти списки загублених карток, «чорні списки», слід хоча б раз у день спеціально виділеній людині оновляти їх в місцях розташування БАК. При значній кількості таких пристроїв подібне обслуговування є складним. Відмова від щоденного оновлення списків може призвести до великих збитків для банку у випадку підробки картки чи при користуванні украденою карткою.

Складності виникають також і за ідентифікації (аутентифікації) клієнта. Для захисту інформації, що зберігається на магнітній картці, застосовується її шифрування. Для того, щоб БАК того самого банку сприймали пластикові картки, у них для шифрування/розшифрування повинен бути використаний один ключ. Компрометація його хоча б на одному з БАК призведе до порушення захисту на всіх БАК.

Крім одиночних сьогодні експлуатуються і мережі БАК, у яких беруть участь кілька банків. Учасники такої мережі ставлять за мету:

– поділ витрат і ризику при розробці нових видів послуг між учасниками мережі;

– зменшення вартості операцій для учасників;

– додання послугам, що робляться, загальнонаціонального характеру, і, відповідно, підвищення їхньої суб'єктивної цінності для споживача;

– можливість для регіональних банків, так само як і для банків, розташованих у фінансових центрах, негайно отримати вигоду від лібералізації законодавства, що регулює вихід на ринки інших країн;

– подолання наявних географічних обмежень, яких не існує для небанківських установ.

При спільному використанні банками мережі БАК з'являється нова проблема – захист конфіденційної інформації кожного із банків (ключі шифрування, списки номерів заборонених до використання карток і т.ін.).

Для захисту взаємодії комп'ютерів банків між собою і з БАК застосовується закінчене шифрування інформації, переданої по лініях зв'язку.

Найчастіше використовується такий метод: уся мережа БАК розбита на зони й у кожній з них використовується свій Головний зональний керуючий ключ. Він призначений для шифрування ключів при обміні між мережним маршрутизатором і головним комп'ютером банку. Ключ індивідуальний для всіх учасників мережі. Звичайно він винятково генерується маршрутизатором і неелектронним способом передається в банк. Розкриття ключа призведе до розкриття всіх PIN, що передаються між маршрутизатором і головним комп'ютером банку.

У неподіленій мережі БАК досить використовувати один відкритий ключ на всіх БАК, а на головному комп'ютері банку закритий. Це дозволить шифрувати запит і підтверджувальне повідомлення та перевіряти дійсність відповідного повідомлення в банку, тому що забезпечення конфіденційності відповідне повідомлення не обов'язково. Особливої уваги потребує проблема захисту запиту від активних атак (зміни введення чи помилкового запиту). Але і вона у випадку неподіленої мережі може бути вирішена з використанням пароля для ідентифікації БАК.

У випадку мережі спільно використовуваних БАК застосування системи шифрування з відкритим ключем дозволяє відмовитися від зональних ключів і дорогої процедури їхньої зміни. Однак у цьому випадку схема ідентифікації БАК за паролем не буде працювати. Ця проблема може бути вирішена в тому випадку, коли кожен БАК разом із запитом буде пересилати і свій відкритий ключ, завірений банком [199, с. 49].

У 90-х рр. XX століття банки перейшли до комп'ютерної обробки інформації, що значно підвищило продуктивність праці, прискорило розрахунки і привело до появи нових послуг. Однак комп'ютерні системи, без яких сьогодні не може обійтися жоден банк, є також джерелом зовсім нових загроз, невідомих раніше. Більшість з них обумовлені новими інформаційними технологіями і не є специфічними винятково для банків.

Сфера інформаційної безпеки – найбільш динамічна галузь розвитку індустрії безпеки в цілому. Якщо забезпечення фізичної безпеки має давню традицію й устояні підходи, то інформаційна безпека постійно вимагає нових рішень, тому що комп'ютерні і телекомунікаційні технології постійно обновляються, на комп'ютерні системи покладається усе більша відповідальність.

Безпека електронних банківських систем залежить від великої кількості факторів, які слід враховувати ще на етапі проектування цієї системи.

При цьому для кожного окремого виду банківських операцій і електронних платежів, інших способів обміну конфіденційною інформацією існують свої специфічні особливості захисту. Таким чином, організація захисту банківських систем – це цілий комплекс заходів, що повинні враховувати як загальні концепції, так і специфічні особливості.

Автоматизація і комп'ютеризація банківської діяльності (і грошового обігу в цілому) продовжує зростати. Основні зміни в банківській індустрії за останні десятиліття пов'язані саме з розвитком інформаційних технологій. Можна прогнозувати подальше зменшення обороту готівки і поступовий перехід на безготівкові розрахунки з використанням пластикових карток, мережі Інтернет і терміналів управління рахунком юридичних осіб.

У зв'язку з цим варто очікувати на подальший динамічний розвиток засобів інформаційної безпеки банків, оскільки їхнє значення постійно зростає.

3.5. Запобігання використанню в злочинних цілях електронних і пластикових платіжних засобів

У БСУ набуває широкого використання такий вид платіжних засобів, як електронні чи пластикові платіжні гроші, а також запроваджена комп'ютеризація міжбанківських розрахунків. Ця обставина сприяла виникненню змін у техніці вчинення низки злочинів у сфері банківської діяльності. Причому тенденція така, щоб чим активніше запроваджуються досягнення техніки та електронні розрахунки у наданні фінансових послуг, тим більш досконалою стає технологія вчинення злочинів з використанням електронних систем, а кількість таких злочинів постійно прогресує.

Вчиненню цих правопорушень сприяють особиста корислива зацікавленість окремих працівників банків, недбале ставлення їх до виконання своїх обов'язків, порушення існуючих правил та інструкцій.

«У матеріалах симпозіуму ООН з питань боротьби з комп'ютерною злочинністю, який проходив у серпні 1990 р. в м.Гавані, відзначалося, що комп'ютерні злочини набувають міжнародного характеру і загрожують економічним основам держав і світовій економічній системі.

У ФРН для боротьби з комп'ютерними злочинами була створена спеціальна служба, яка у 1984 р. зареєструвала 222 інформації про протиправну діяльність у цій сфері, а роком пізніше – 695 комп'ютерних правопорушень. У Нідерландах у 1989 р. порівняно з 1988 р. комп'ютерні

злочини подвоїлись. Якщо 30 років тому у США було зареєстровано перший комп'ютерний злочин, то на початку 1984 року таких злочинів налічувалось 1200. Ці відомості підтверджують стійку тенденцію поширення комп'ютерної злочинності.

На погляд зарубіжних спеціалістів, злочинний світ у близькому майбутньому може відмовитися від пограбувань банків, оскільки незаконне використання комп'ютерних систем у разі проведення банківських операцій дає більші прибутки з меншим ризиком» [133, с. 268–269].

Статистика таких злочинів велася з 1958 р. Тоді під ними малися на увазі: випадки псування і розкрадання комп'ютерного устаткування; крадіжка інформації; шахрайство чи крадіжка грошей, проведенні із застосуванням комп'ютерів; несанкціоноване використання комп'ютерів чи крадіжка машинного часу. Записи велися у Стенфордському дослідницькому інституті і тривалий час не становили великого інтересу. До речі, у 1966 р. комп'ютер вперше використаний як інструмент для пограбування банку в Міннесоті [187].

У наші дні в зв'язку із загальною інформатизацією і комп'ютеризацією банківської діяльності значення інформаційної безпеки банків значно зросло. Ще 30 років тому об'єктом інформаційних устремлінь були дані про клієнтів банків чи про діяльність самого банку. Сьогодні у результаті повсюдного поширення електронних платежів, пластикових карт, комп'ютерних мереж об'єктом інформаційних злочинів стали безпосередньо кошти як банків, так і їхніх клієнтів. Зробити спробу розкрадання може кожен – необхідна лише наявність комп'ютера, підключеного до мережі Інтернет. Причому для цього не потрібно фізично проникати в банк, можна «працювати» і за тисячі кілометрів від нього.

Наприклад, у серпні 1995 р. у Великій Британії був заарештований 24-літній російський математик Володимир Левін, який за допомогою свого домашнього комп'ютера в Петербурзі зумів проникнути в банківську систему одного з найбільших американських банків Citibank і викрасти $ 2,8 млн У 1994 році Левін разом із приятелем зумів підібрати ключі до системи банківського захисту Citibank і спробував зняти з його рахунків великі суми. За даними московського представництва Citibank, досі подібне нікому не вдавалося. Служба безпеки Citibank з'ясувала, що в банку намагалися викрасти $ 2,8 млн, але контролюючі системи вчасно це розпізнали і заблокували рахунки. Украсти вдалося лише $ 400 тис. Для отримання грошей Левін виїхав в Англію, де і був заарештований [191].

Комп'ютеризація банківської діяльності дозволила значно підвищити продуктивність праці співробітників банку, упровадити нові фінансові продукти і технології. Однак прогрес у техніці злочинів йшов не менш швидкими темпами, ніж розвиток банківських технологій. Сьогодні понад

90% усіх злочинів пов'язані з використанням автоматизованих систем обробки інформації банку (АСОІБ) [192, с. 17]. Отже, при створенні і модернізації АСОІБ банкам необхідно приділяти пильну увагу забезпеченню її безпеки.

Саме ця проблема є зараз найактуальнішою й найменш дослідженою. Якщо в забезпеченні фізичної та класичної інформаційної безпеки давно вже вироблені підходи (під класичною інформаційною безпекою розуміють систему розподілу прав доступу до інформації, заходи щодо захисту від прослуховування, попередження витоків інформації з боку персоналу й інші методи, не пов'язані з АСОІБ), то в зв'язку з частими радикальними змінами в комп'ютерних технологіях методи безпеки АСОІБ вимагають постійного удосконалення. Як показує практика, не існує складних комп'ютерних систем, які не містять помилок. А оскільки ідеологія побудови великих АСОІБ регулярно змінюється, виправлення знайдених помилок і «дірок» у системах безпеки вистачає ненадовго, тому що кожна нова комп'ютерна система утворює нові проблеми і нові помилки та змушує по-новому перебудовувати систему безпеки.

Особливо актуальна порушена проблема в Україні. У західних банках програмне забезпечення (ПЗ) розробляється конкретно під кожен банк і пристрій АСОІБ і є комерційною таємницею. В Україні поширені «стандартні» банківські пакети, інформація про які широко відома, що полегшує несанкціонований доступ у банківські комп'ютерні системи. У процесі розвитку й розширення сфери застосування засобів обчислювальної техніки гострота проблеми забезпечення безпеки обчислювальних систем і захисту збереженої й обробленої в них інформації від різних загроз усе більше зростає. Для цього існує низка об'єктивних причин. Основна з них – рівень довіри до автоматизованих систем обробки інформації. Їм довіряють саму відповідальну роботу, від якості якої залежить життя і добробут багатьох людей. ЕОМ виконують фінансові операції, обробляють секретну інформацію.

Сьогодні проблема захисту обчислювальних систем стає ще більш значною у зв'язку з розвитком і поширенням мереж ЕОМ. Розподільні системи і системи з обмеженим доступом висунули на перший план питання захисту обробленої та переданої інформації.

Цілісну систему захисту створити досить складно, оскільки досі немає єдиної теорії захисту комп'ютерних систем. Існує багато підходів і точок зору на методологію її побудови. У цьому напрямі докладаються серйозні зусилля як у практичному, так і в теоретичному плані, використовуються самі останні досягнення науки, залучаються передові технології. Цією проблемою займаються правові фірми з виробництва комп'ютерів і програмного забезпечення, інститути, а також великі банки та міжнародні корпорації.

Використовуються різні варіанти захисту інформації – від охоронця на вході до математично вивірених засобів приховування даних від ознайомлення. Сьогодні можна говорити про глобальний захист і його окремі аспекти: захист персональних комп'ютерів, мереж, баз даних тощо. З'ясовано, що абсолютно захищених систем немає. Можна говорити про надійність системи, по-перше, лише з певною імовірністю, а, по-друге, тільки про захист від визначеної категорії порушників. І все ж проникнення в комп'ютерну систему можна передбачити. Захист – це свого роду змагання оборони й нападу: хто більше знає і передбачає дійові заходи, той і виграє.

Сучасний банк важко уявити без автоматизованої інформаційної системи. Комп'ютер на столі банківського службовця вже давно перетворився у звичний і необхідний інструмент. Зв'язок комп'ютерів між собою та з більш могутніми комп'ютерами, а також з ЕОМ інших банків – також необхідна умова успішної діяльності банку. Занадто велика кількість операцій, які необхідно виконати в плині короткого періоду часу.

Оцінки втрат від злочинів, пов'язаних із втручанням у діяльність інформаційної системи банків, дуже сильно різняться. Відзначається різноманітність методик для їхнього підрахунку. Середня банківська крадіжка із застосуванням електронних заходів складає близько $ 9.000, а один з найгучніших скандалів пов'язаний зі спробою украсти $ 700 млн (Перший національний банк, Чикаго) [193, с. 56].

Тут слід враховувати не тільки суми прямого збитку, але й дуже дорогі заходи, що проводяться після успішних спроб злому комп'ютерних систем. Так, недавня пропажа даних про роботу із секретними рахунками Bank of England у січні 1999 р. змусила банк поміняти коди всіх кореспондентських рахунків. У цьому зв'язку у Великій Британії були підняті по тривозі всі наявні сили розвідки і контррозвідки для того, щоб не допустити неймовірного витоку інформації, здатної завдати величезної шкоди. Урядом вживаються крайні заходи для того, щоб стороннім не стали відомі рахунки й адреси, за якими Bank of England направляє щодня сотні мільярдів доларів. Причому у Великій Британії більше побоювалися ситуації, за яких дані могли потрапити в розпорядження іноземних спецслужб. У такому випадку була б розкрита уся фінансова кореспондентська мережа Bank of England. Можливість збитку була ліквідована протягом кількох тижнів [191].

Рівень оснащення засобами автоматизації відіграє важливу роль у діяльності банку і відображається на його доходах. Чим менше часу будуть займати розрахунки між банком і клієнтами, тим вищим стане банківський обіг, а отже, прибуток.

Сьогодні АСОІБ банку є одним з найбільш уразливих місць у всій організації, що притягає зловмисників як ззовні, так і з числа співробітників

самого банку, про що свідчать такі факти: втрати банків й інших фінансових організацій від впливом на їхні системи обробки інформації становлять близько $ 3 млрд на рік; обсяг втрат, пов'язаних з використанням пластикових карток оцінюється в $ 2 млрд на рік, що складає 0,03-2% від загального обсягу платежів залежно від використовуваної системи [193, с. 60].

Один з найгучніших скандалів пов'язаний зі спробою сімох чоловік украсти $ 700 млн (попереджено ФБР) у Першому національному банку Чикаго; 27 млн фунтів стерлінгів були украдені з Лондонського відділення Union Bank of Switzerland; DM 4 млн украдені з Chase Bank (Франкфурт) – службовець переказав гроші в банк Гонконгу, вони були узяті з великої кількості рахунків, крадіжка виявилася успішною; $ 3 млн украдені в банку Стокгольма, крадіжка була проведена з використанням привілейованого становища декількох службовців в інформаційній системі банку і також виявилася успішною [194].

Для запобігання таким крадіжкам більшість банків вживають необхідних заходів захисту, серед яких важлива роль належить АСОІБ. Як свідчить досвід, захист АСОІБ банку – дорогий і складний захід. Так, наприклад, Barclays Bank витрачає на захист своєї автоматизованої системи близько $ 20 млн щорічно [196].

Стратегія інформаційної безпеки банків дуже відрізняється від аналогічних стратегій інших компаній і організацій. Це зумовлено насамперед специфічним характером загроз, а також публічною діяльністю банків, які змушені робити доступ до рахунків досить легким для зручності клієнтів.

Інформаційна безпека банку має враховувати такі специфічні фактори:

– накопичена в банківських установах інформація являє собою реальні гроші. На основі інформації комп'ютера можуть відкриватися кредити, переводитися значні суми. Ця особливість різко розширює коло злочинців;

– інформація в банківських системах торкається інтересів великої кількості людей і організацій – клієнтів банку. Як правило, вона конфіденційна, і банк несе відповідальність за забезпечення певного ступеня таємності перед своїми клієнтами;

– конкурентоздатність банку залежить від того, наскільки клієнту зручно працювати з банком. Така легкість доступу до грошей підвищує імовірність злочинного проникнення до банківських рахунків;

– інформаційна безпека банку (на відміну від більшості компаній) повинна забезпечувати високу надійність роботи комп'ютерних систем навіть у випадку позаштатних ситуацій, оскільки банк несе відповідальність не тільки за свої заходи, але й за гроші клієнтів.

Злочини в банківській сфері також мають свої особливості [186, с. 16]:

– багато злочинів, вчинених у банківській сфері, залишаються невідомими для широкої публіки у зв'язку з тим, що керівники банків не хочуть турбувати своїх акціонерів, бояться піддати свою організацію новим злочинам, побоюються «підмочити» репутацію надійного сховища заходів і, як наслідок, втрати клієнтів;

– як правило, зловмисники звичайно використовують свої власні рахунки, на які переводяться викрадені суми. Більшість злочинців не знають як «відмити» украдені гроші. Уміння вчинити злочин і уміння отримати гроші – це не одне і те саме;

– більшість комп'ютерних злочинів – дрібні. Збитки від них коливаються в інтервалі від $ 10.000 до $ 50.000;

– успішні комп'ютерні злочини, як правило, вимагають великої кількості банківських операцій (кілька сотень). Однак великі суми можуть пересилатися і всього за кілька трансакцій;

– комп'ютерні злочини не завжди високотехнологічні. Досить підробки даних, зміни параметрів середовища АСОІБ тощо, а ці дії доступні й обслуговуючому персоналу;

– багато зловмисників пояснюють свої дії тим, що вони усього лише беруть у борг у банку з наступним поверненням. Втім «повернення», як правило, не відбувається.

Специфіка захисту автоматизованих систем обробки інформації банків (АСОІБ) зумовлена особливостями завдань, які вони покликані вирішувати:

– як правило, АСОІБ обробляють великий потік запитів, що постійно надходять у реальному масштабі часу, кожний з яких не вимагає для обробки численних ресурсів, але всі вони мусять бути оброблені тільки високопродуктивною системою;

– в АСОІБ зберігається й обробляється конфіденційна інформація, не призначена для широкої публіки. Її підробка чи витік можуть призвести до серйозних (для банку чи його клієнтів) наслідків. Тому АСОІБ приречені залишатися відносно закритими, працювати під управлінням специфічного програмного забезпечення і приділяти велику увагу забезпеченню своєї безпеки;

– підвищені вимоги до надійності апаратного і програмного забезпечення, що дозволяє проводити беззупинну обробку інформації навіть за умови різних збоїв і відмов;

– аналітичні завдання – планування, аналіз рахунків і т.ін. Вони не є оперативними і вимагають тривалого часу для розв'язання, а їхні результати можуть вплинути на політику банку у відношенні конкретного клієнта чи проекту. Тому підсистема, яка забезпечує та враховує аналітичні завдання, повинна бути надійно ізольована від основної системи обробки інформації;

– завдання, які розв'язуються у щоденній діяльності, у першу чергу, виконання платежів і корегування рахунків. Саме вони й визначають розмір та потужність основної системи банку; для їхнього вирішення звичайно потрібно набагато більше ресурсів, ніж для аналітичних завдань. У той же час, цінність інформації, обробленої за розв'язання таких завдань, має тимчасовий характер. Поступово вона (наприклад, про виконання будь-якого платежу) стає не актуальною. Тому інколи достатньо забезпечити захист платежу саме в момент його проведення. При цьому захист самого процесу обробки і кінцевих результатів має бути постійним.

Яким заходам систем обробки інформації віддають перевагу закордонні фахівці? На це питання можна відповісти, використовуючи результати опитування, проведеного Datapro Information Group у 1994 р. серед банків і фінансових організацій [186]:

– сформовану політику інформаційної безпеки мають 82% опитаних. Порівняно з 1991 р. відсоток організацій, що мають систему безпеки, збільшився на 13%;

– 12% опитаних планують розробити політику безпеки;

– у 88% організацій, що мають політику інформаційної безпеки, існує спеціальний підрозділ, який відповідає за її реалізацію;

– у плані захисту особлива увага приділяється захисту комп'ютерних мереж (90%), великих ЕОМ (82%), відновленню інформації після аварій і катастроф (73%), захисту від комп'ютерних вірусів (72%), захисту персональних ЕОМ (69%).

Із зазначеного випливають висновки щодо особливості захисту інформації в закордонних фінансових системах [186, С.21]: головне в захисті фінансових організацій – оперативне і якнайповніше відновлення інформації після аварій і збоїв; наступна за важливістю для фінансових організацій проблема – це управління доступом користувачів до збереженої й оброблюваної інформації. До відмінностей про організацію захисту мереж ЕОМ у фінансових організаціях можна віднести широке використання стандартного (тобто адаптованого, але не спеціально розробленого для конкретної організації) комерційного програмного забезпечення для управління доступом до мережі (82%), захист точок підключення до системи через лінії зв'язку, що комутуються (69%). Значна увага у фінансових організаціях надається фізичному захисту приміщень, у яких розташовані комп'ютери (близько 40%), та шифрування локальної інформації застосовують трохи більше 20% фінансових організацій. Причинами цього є складність поширення ключів, суворі вимоги до швидкості дії системи, а також потреба у оперативному відновленні інформації у разі збоїв і відмовлень устаткування. Значно менша увага у фінансових організаціях надається захисту телефонних ліній зв'язку (4%).

Аналіз наведеної статистики дозволив зробити важливий висновок: системи захисту фінансових організацій (у тому числі й банків) створюється трохи інакше, ніж звичайних комерційних і державних організацій. Отже для захисту АСОІБ не можна застосовувати ті самі технічні й організаційні рішення, що були розроблені для стандартних ситуацій. Не можна бездумно копіювати чужі системи – вони розроблялися для інших умов.

Для того, щоб залишитися конкурентоздатними в XXI столітті банки повинні оцінювати зовнішні фактори й адекватно реагувати на них. До того ж на діяльність банків впливають і внутрішні фактори такі, як зміна запитів клієнтів, потреба у зменшенні часу обслуговування, розширенні використання високих технологій.

До основних зовнішніх факторів, що впливають на банківську індустрію в Європі, фахівці [195, С.42] відносять такі:

– загальний ринок, оскільки Європейське Співтовариство прийняло рішення про створення Загального європейського ринку товарів і послуг, яке впливає на діяльність банків;

– найзначнішим актом, що впливає на діяльність банків, є Друга координаційна банківська директива [Second Coordination Directive (Banking)], прийнята до виконання всіма членами Співтовариства з 1 січня 1993 р. Основним змістом цієї директиви є принципи внутрішньодержавного управління і загального схвалення членами Співтовариства стандартів контролю та регулювання діяльності банків. Це дозволяє банкам Співтовариства, що має ліцензії на діяльність у своїй країні, виконувати операції в межах усього Співтовариства без одержання додаткових ліцензій;

– глобалізація ринку послуг. З розвитком нових технологій зникають обмеження, пов'язані з національними бар'єрами, і ринок послуг стає доступним 24 години на добу;

– зміни в законодавстві. Ці зміни заохочують небанківські організації робити фінансові послуги в прямому суперництві з банками. Небанківські організації використовують мережу клієнтів, що розширюється, і збільшення продаж у тих сферах, що були винятково вотчиною банків. Так, наприклад, англійська фірма Marks & Spencer успішно впровадилася на фінансовий ринок за допомогою створення власного інвестиційного фонду і карток для обслуговування в магазинах;

– посилення вимогливості клієнтів. Інформованість клієнтів про доступність послуг банків і їхню вартість призводить до посилення вимог до якості й вартості запропонованих послуг. Клієнти також прекрасно поінформовані про ризик, пов'язаний з банківською діяльністю, і стають більш обережними при вкладенні грошей у ненадійні банки;

– обробка трансакцій залишається найбільш трудомістким елементом низки пріоритетів банку; вона повинна бути безпомилковою та забезпечувати точну і своєчасну інформацію;

– Технології. За останнє десятиліття розвиток технологій заходів обробки й передачі інформації допоміг збільшити продуктивність і зменшити вартість банківських операцій. Сучасні технології дозволяють практично моментально отримувати й використовувати інформацію про клієнтів, продукти і ризики, що, безсумнівно, впливає на конкурентноздатність банків. Однак поки далеко не всі банки повною мірою використовують ці можливості. Засоби телекомунікацій разом з новими інформаційними технологіями стають інструментом для розробки нових продуктів і механізмів їхнього розповсюдження, що розширює сферу діяльності банків. Електронні платежі і засоби розрахунку в точці продажу – приклади використання нових технологій, що докорінно змінюють банківську індустрію.

Сучасні технології є альтернативою традиційним банківським продуктам і послугам. Зміни, що призвели до зменшення обсягу локальних операцій, перебувають в центрі уваги. Так, Deutsche Bank у 1992 р. оголосив про збитки, пов'язані з обслуговуванням приватних осіб, у сумі DM 200 млн. Проте він продовжував виконувати програму розширення мережі самообслуговування шляхом емітування 3-х млн електронних карт [195, с. 51].

Використання сучасних технологій створило новий ринок, де технології стають товаром у таких сферах, як обмін електронними даними, системи електронних платежів у точці продажу тощо. Насамперед це стосується поліпшення обслуговування клієнтів і надання більш специфічних послуг.

Зростає потреба жорсткого контролю за витратами, особливо в умовах збільшення витрат на регулювання діяльності та появи на ринку нових дешевих товарів і послуг, вироблених небанківськими організаціями. Такий контроль може бути проведений за допомогою централізованої обробки інформації й удосконалювання управління. Підвищується необхідність обробки постійно зростаючого потоку інформації про стан ринку для більш точного визначення місця специфічної продукції на ринку, що розширюється.

Застосування нових технологій впливає на стратегічні напрямки і напрямки бізнесу в діяльності банку. Банки здавна впроваджують і використовують найсучасніші досягнення науки і техніки для полегшення ручної праці та прискорення виконуваних операцій. Однак зараз цього вже недостатньо і переможцями будуть ті, хто цілком видозмінить свою діяльність відповідно до сучасних технологій. Розвиток сучасних

інформаційних технологій може провадитися під впливом бізнесу і для бізнесу. Особливо важливим у цьому процесі є те, що інформаційні технології розвиваються в тісній взаємодії з економікою. Інформаційні технології впливають на розмір одержуваних доходів і на те, як вони накопичуються і розподіляються.

Інформаційні технології пронизують кожен елемент низки пріоритетів банку, наповнюючи їх новим змістом і впливаючи на зв'язок елементів між собою. Крім того, технології впливають на конкурентноздатність банків, змінюючи життєвий цикл продукції, запропонованої клієнтам. Стратегії застосування інформаційних технологій визначають методи, за допомогою яких вони змінюють сучасний бізнес, і шляхи управління цими змінами. Важливим моментом є розробка архітектури комп'ютерної системи банку. Під архітектурою системи розуміється сукупність її функціональних компонентів і їхня взаємодія один з одним. Метою розробки архітектури комп'ютерної системи банку є створення внутрішньологічної і гнучкої системи, що буде впливати на зміни стратегії діяльності банку з мінімальним впливом на неї. Будь-яка архітектура має сполучатися зі стратегією банку і спрощувати втілення її в життя.

Це напрям особливо важливий при розробці взаємних угод між організаціями та у разі їхнього злиття. Наприклад, злиття Dutch Postbank і Naturale Nederlanden, англійських Lloyds Abbey Life, німецьких – Deutsche Bank Deutsch Lebensversicherung – призвело до виникнення проблем, пов'язаних з інформаційними технологіями. Завдання полягає у тому, щоб розробити таку архітектуру, що поєднає критичну діяльність клієнтів і канали розподілу товарів та послуг банку, не порушуючи при цьому порядку роботи організацій [195. с. 60].

Багато в чому прибутковість банку залежить від забезпечення вищого керівництва потрібною, своєчасною і точною інформацією. Системи управління інформацією мають бути справжніми помічниками в діяльності банку, забезпечуючи, наприклад, інформацією про положення на ринку, прибутковість банківської продукції, становище клієнтів тощо. Отримана з їх допомогою інформація може використовуватися банком для поліпшення обслуговування клієнтів чи для представлення їм з метою використання у власних інтересах.

Банкам потрібна постійна інформація про ступінь ризику їхньої діяльності. Оцінка ризику – це процес, що докорінно може бути змінений за допомогою сучасних технологій. У нього можуть бути залучені більш «інтелектуальні» системи, що здатні оцінювати відсоткові ставки, курси валют, кредитоспроможність клієнта і т.ін., видаючи при цьому рекомендації щодо можливих дій та їхніх результатів.

Сучасні технології дають банкам величезні переваги в організації систем доставки товарів і послуг. Використання електронних засобів зв'язку

дозволяє реалізувати: електронні платежі та розрахунки в точці продажу; клієнтські термінали, що мають прямий зв'язок з банком; домашнє банківське обслуговування за допомогою персонального комп'ютера чи телефону; обмін електронними даними в мережі з розширеним набором послуг; технології електронних банківських карт, включаючи магнітні пластикові й інтелектуальні карти.

Реалізація цих й інших методів банківського обслуговування в конкретних системах вимагає розробки жорстких заходів захисту для запобігання випадкових і навмисних порушень їхнього функціонування. Одна з важливих проблем банків сьогодні – це управління інвестиціями в електронні банківські системи для того, щоб останні цілком відбивали зміни в банківській індустрії. Успіх на нових стратегічних напрямах бізнесу багато в чому залежить від реалізації інформаційних систем.

Протидія комп'ютерній злочинності передбачає, перш за все створення відповідної законодавчої бази, комплексу організаційних заходів, у тому числі підготовку кадрів високої кваліфікації, а також відповідне спеціальне технічне забезпечення.

Із входженням України до Європейського Співтовариства та підписанням 23 листопада 2001 р. Європейської конвенції про кіберзлочинність, у якій чітко визначені види комп'ютерної злочинності та шляхи взаємодії урядів щодо боротьби з ними, виникла нагальна потреба реформування чинного законодавства. Відсутність міждержавних кордонів у глобальних інформаційних мережах є однією з основних особливостей, які потрібно враховувати при протидії та профілактиці комп'ютерних правопорушень.

Комітет у справах законодавства Ради Європи рекомендує уніфікувати кримінальне законодавство з питань комп'ютерних правопорушень та передбачити відповідальність за такі злочини: незаконний доступ (доступ до інформації без відповідної санкції або з порушенням його правил); нелегальне перехоплення інформації (технічними засобами комп'ютерної інформації чи перехоплення комп'ютерних випромінювань); втручання у дані (знищення, зміна або приховування інформації); втручання у систему (перешкоджання функціонуванню комп'ютерної системи); зловживання пристроями (виготовлення та розповсюдження пристроїв для вчинення комп'ютерних злочинів); підробка, пов'язана з комп'ютерами (дії для створення недійсних даних); шахрайство, пов'язане з комп'ютерами (дії, що призводять до втрати майна іншої особи внаслідок втручання у комп'ютерні системи); комп'ютерне шахрайство (втручання у роботу інформаційної системи з метою отримання економічної вигоди); розповсюдження дитячої порнографії; правопорушення, пов'язані з авторським правом.

Конвенцією передбачена також потреба у прийнятті низки процедурних питань стосовно виявлення та документування комп'ютерних злочинів. Протидія комп'ютерній злочинності потребує принципово нових напрацювань щодо методології досудового розслідування. Зокрема, ст.16 Конвенції встановлює, що кожна сторона вживає таких законодавчих та інших заходів, які можуть бути необхідними для надання можливості своїм компетентним органам видавати накази або іншим шляхом забезпечувати збереження комп'ютерних даних, включаючи відомості про рух інформації.

Зазначені положення у країнах Європейського Союзу врегульовані згідно з Резолюцією Ради про оперативні запити правоохоронних органів стосовно телекомунікаційних мереж загального користування та послуг від 20 червня 2001 р. № 9194/01 та Резолюцією Ради про законне перехоплення телекомунікацій від 17 січня 1995 р. № 96/С 329/01 [188, с. 116].

Реалії сьогодення вимагають активного формування відповідних підрозділів у МВС, СБУ, ДПА України. Наприклад, створення у 2001 р. Управління по боротьбі зі злочинами у сфері високих технологій МВС України дало можливість викривати злочини та порушувати кримінальні справи щорічно у кілька разів більше, ніж за всі попередні роки з моменту введення кримінальної відповідальності за них (1994 р.) [189]. Діяльність цих підрозділів потребує координації з боку спеціально створеного органу, адже кіберзлочини стосуються і неправомірного доступу до таємної інформації, і крадіжок коштів з пластикових карток та електронних рахунків банків, і ухилення від сплати податків, а також – використання електронних засобів терористами.

З метою ефективної протидії кіберзлочинності Указом Президента України «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» № 193/2001 від 6 грудня 2001 р. передбачено створення Міжвідомчого центру з питань боротьби з комп'ютерною злочинністю.

Підтримуючи пропозицію Кабінету Міністрів України щодо його відкриття, вноситься пропозиція зазначений підрозділ створити у структурі Координаційного комітету по боротьбі з корупцією і організованою злочинністю, який відповідно до ст. 8 Закону «Про організаційно-правові основи боротьби з організованою злочинністю» від 30 червня 1993 р. координує діяльність всіх державних органів, що ведуть боротьбу з організованою злочинністю, у тому числі з комп'ютерною. Наукове, аналітичне та інформаційне забезпечення покласти на Міжвідомчий НДЦ з проблем боротьби з організованою злочинністю за умови відповідного штатного та фінансового забезпечення [188].

На відповідний Центр у Великій Британії покладено виконання таких завдань: діяльність проти організованої злочинності транснаціонального характеру та у сфері високих технологій; проведення стратегічних прогнозів; проведення розслідувань; координація діяльності правоохоронних органів; розроблення рекомендацій для правоохоронних органів.

У структурі Центру чотири відділи: розслідування – проводить розслідування й підтримує інші правоохоронні органи у розслідуванні тяжких та вчинених організованими групами злочинів з використанням високих технологій; розвідки – забезпечує стратегічну і тактичну розвідку та співробітництво із зарубіжними партнерами; тактичної і технічної підтримки – забезпечує консультативну підтримку та допомогу місцевим правоохоронним агентствам, міжнародним правоохоронним організаціям, уряду і промисловості; цифрових доказів – забезпечує судову підтримку при розгляді злочинів у сфері високих технологій [188, С.117].

За прогнозами провідних науковців у галузі інформаційної безпеки, вже найближчими роками можливе стрімке зростання кількості кіберзлочинів. Так, за розрахунками компанії Gartner, вже у кінці 2004 р. економічні збитки від них збільшаться у 10–100 разів [190].

Тому Україна також повинна зробити відповідні кроки щодо своєї інформаційної безпеки, яка згідно з Конституцією є невід'ємною складовою національної безпеки нашої держави.

Стосовно поняття злочинів у сфері комп'ютерної інформації слід зазначити таке. В Україні кримінальна відповідальність за посягання у сфері комп'ютерної інформації (її ще називають «комп'ютерна» або «кіберзлочинність») була встановлена лише у 1994 р.

За даними статистики МВС України протягом 1997–2000 р. зареєстровано 36 злочинів у сфері комп'ютерної інформації. Протягом 2001 р. органами внутрішніх справ було виявлено 16 таких злочинів, а у 2002 р. – вже 30. Слід враховувати, що невеликі статистичні показники зумовлені злочинами, які характеризуються надзвичайно високим ступенем латентності.

У новому КК України існує три статті, що передбачають відповідальність за злочини аналізованого виду. Вони об'єднані розділом XVI Особливої частини, який має назву «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». КК України містить й інші статті, які можуть застосовуватися при визначенні відповідальності за вказані посягання. Зокрема, ч.3 ст.190 (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки) і ст. 200 (використання підроблених електронних засобів доступу до банківських рахунків) [178, с. 86].

Україна відстає у створенні відповідної нормативної бази. Навіть у Комплексній програмі профілактики злочинності на 2001–2005 рр. жодним словом не згадується про злочини у цій сфері. І це при тому, що Концепція національної безпеки України затверджена постановою Верховної Ради від 16 січня 1997 р., називає основними загрозами національній безпеці загрози в інформаційній сфері. Однією з них є невиваженість державної політики та відсутність необхідної інфраструктури у названій сфері.

В Україні серйозних наукових розробок проблем небезпечних діянь у сфері комп'ютерної інформації та кримінологічних проблем запобігання цим злочинам немає. У небагатьох публікаціях на вказану тему неконкретно розглядається коло питань, пов'язаних зі злочинами зазначеного виду.

Існує три основні підходи до визначення злочинів у цій сфері.

Прихильники першої позиції злочинами у сфері комп'ютерної інформації вважають усі суспільно небезпечні діяння, предметом яких є комп'ютерна інформація [179, с. 9]. Згідно з іншою точкою зору, злочини слід вважати комп'ютерними у тому разі, коли інформація (інформаційні технології) є знаряддям їх вчинення [180, с. 6]. Нарешті, останній підхід полягає у визнанні злочинами у сфері комп'ютерної інформації лише тих посягань, і предметом, і знаряддям вчинення яких є комп'ютерна інформація [181, с. 148].

Отже, всі дослідники як критерії, що дають можливість відмежувати злочини у названій сфері від інших посягань, у різних комбінаціях використовують ознаки предмета злочину і знарядь його вчинення.

Окремі науковці вважають за доцільне дещо розширити загальнотеоретичне поняття предмета злочину [182, с. 75–78; 183, с. 87]. Тому пропонується включити не тільки речі матеріального світу, а й певні, об'єктивно існуючі, явища утворення – комп'ютерну інформацію. «Тоді вирішується значна кількість теоретичних проблем щодо визначення останнього не лише у складах злочинів у сфері комп'ютерної інформації, а й у деяких інших (загалом у кримінальному законодавстві існує близько 30 норм, у яких інформація в різних її проявах прямо названа тим матеріальним утворенням, впливаючи на яке винний заподіює шкоду об'єктові)» [178, с. 87].

Різновидом комп'ютерної інформації є комп'ютерні програми.

Висловлюється цілком слушна думка, що «єдиний правильний підхід до створення загального поняття злочинів у вказаній сфері полягає у одночасному врахуванні (як їхніх ознак) предмета і знарядь вчинення цих посягань. Спираючись тільки на таке поєднання ознак складу злочину, можна створити «формулу», яка дозволила б безпомилково відрізняти злочини у названій сфері від інших суспільно небезпечних діянь.

Особливість аналізованих посягань у тому, що вони вчиняються у віртуальному просторі. У ньому набуває вияву суспільно небезпечне діяння, починають проявлятися суспільно небезпечні наслідки і навіть знаряддя вчинення злочину є віртуальними... Сутність механізму вчинення злочинів у сфері комп'ютерної інформації полягає у тому, що винний використовує одну комп'ютерну інформацію (знаряддя) для злочинного впливу на іншу комп'ютерну інформацію (предмет). Саме такий механізм надає цим посяганням виключної специфічності, яка, зокрема, зумовлює необхідність створення спеціальних кримінально-правових норм про відповідальність за злочини у сфері комп'ютерної інформації [178, С.88].

Не маючи заперечення щодо того, що комп'ютерні злочини у БСУ мають свою специфіку, слід зазначити, що названа інформація є лише предметом або тільки знаряддям вчинення злочину, останній має кваліфікуватися залежно від спрямованості умислу винного та фактичних наслідків вчиненого. «Відповідальність за такі діяння з урахуванням усіх інших обставин може наставати за різними статтями КК України, зокрема: 109, 110, 111, 114, 132, 145, 163, 176, 177, 182, 199, 215, 216, 224, 231, 232, 238, 259, 300, 301, 318, 328, 330, 358, 359, 381, 387, 422, 436.

Подібні думки рідко, але зустрічаються у науковій літературі, однак їх автори зупиняються у своїх міркуваннях і вважають достатнім при створенні визначення злочинів у сфері комп'ютерної інформації врахувати лише дві ознаки останніх – предмет і знаряддя. Ми не поділяємо наведеної точки зору, що пояснюється декількома обставинами» [178, с. 88].

Ми поділяємо думку авторів, що предметом, стосовно якого виникають суспільні відносини, є комп'ютерна інформація, суб'єктами – будь-які фізичні та юридичні особи. «Отже, родовим об'єктом аналізованих посягань потрібно визнати суспільні відносини у сфері комп'ютерної інформації. З огляду на зазначене видається за доцільне викласти назву розділу XVI Особливої частини КК України так: «Злочини у сфері комп'ютерної інформації», оскільки теперішня не відбиває сутності родового об'єкта злочинів, відповідальність за які передбачена статтями, що їх об'єднано у зазначеному розділі.

Слід також згадати форму вини, з якою вчиняються злочини у сфері комп'ютерної інформації. Для останніх характерною є лише умисна форма. Вважаємо, що саме умисна форма вини є однією з основних ознак злочинів у цій сфері, яка повинна враховуватися при створенні теоретичного визначення таких суспільно небезпечних діянь. Необережне вчинення посягання, яке певним чином пов'язане з комп'ютерними системами і телекомунікаційними мережами, має, на нашу думку, кваліфікуватися за іншими, загальними, нормами КК України...

Таким чином, злочини у сфері комп'ютерної інформації – це протиправні умисні суспільно небезпечні діяння, котрі посягають на відносини щодо здійснення інформаційної діяльності стосовно комп'ютерної інформації, предметом і знаряддям вчинення яких є така інформація. Остання може існувати у різних проявах – відомості, дані, комп'ютерні програми тощо [178, с. 89].

Ці автори справедливо наголошують на тому, що питання, пов'язані із застосуванням норм про кримінальну відповідальність за злочини у сфері комп'ютерної інформації, потребують роз'яснення Пленуму Верховного Суду України у відповідній постанові. У ній доцільно приділити увагу роз'ясненню окремих термінів і термінологічних зворотів, які використовуються у формулюваннях аналізованих кримінально-правових заборон, основним проблемам кваліфікації злочинів у сфері комп'ютерної інформації, питанням призначення покарання тощо.

Практика засвідчує, що комп'ютерні злочини умовно поділяються на чотири основних види: шахрайство і маніпуляції з інформаційною технікою; незаконне використання машинного часу; розкрадання програм (економічне шпигунство) та комп'ютерний саботаж.

До шахрайства і маніпуляцій з інформаційною технікою відноситься неправомірна заміна носіїв інформації та програмного забезпечення, а також несанкційований доступ до процесу обробки відомостей.

Незаконне використання машинного часу полягає у неправомірному використанні у своїх особистих цілях ЕОМ.

До комп'ютерного саботажу відноситься: стирання, приведення у непридатний стан або фальсифікація інформації, пошкодження засобів інформаційної техніки, нав'язування захисту комп'ютерних систем і комп'ютерне вимагання (різновидність рекету), користуючись недосконалістю технічного захисту комп'ютерних систем.

У західній практиці таким злочинам надаються умовні назви.

Наприклад, «повітряний змій» – коли клієнт або операційний працівник банку відкриває два рахунки у різних банківських установах і депонує грошові кошти з одного рахунку на інший і назад, постійно збільшуючи суми. Коли набралась велика сума, відомості про джерела утворення цих сум з пам'яті ЕОМ стираються.

При способі розкрадання «з миру по нитці» – зловмисник, маючи доступ до рахунку клієнта, у якого є великі залишки коштів на рахунку, або який виконує розрахункові операції на великі суми, перераховує з них відносно невеликі суми на інший рахунок, звідки їх знімає. Для власника рахунку вони є незначними і не поміченими.

Перший спосіб розкрадання нагадує відомі у нас злочини, коли зловмисники переганяють і «відмивають» фіктивно утворені суми за

допомогою псевдоугод, фіктивних кредитових авізо, чекових книжок, акредитива.

«Строки покарання за такі дії залежно від небезпечності злочину у різних країнах визначаються по-різному. У Швейцарії за менш небезпечні факти «відмивання» грошей передбачено два роки ув'язнення, за важкі – 5, у Німеччині – відповідно 5 і 10 років. В Англії двома роками позбавлення волі карається також відсутність у фірмі заходів щодо процедури викриття фактів «відмивання» грошей, здобутих злочинним шляхом.

Приблизно 80-90% вчинених у ФРН комп'ютерних злочинів правоохоронним органам залишаються невідомими [133, с. 270–273].

Слід підкреслити, що при покаранні злочинців з фінансових установ за «відмивання» грошей правоохоронним органам не потрібно доказувати, що гроші були здобуті злочинним шляхом, тобто карається сама процедура неналежної перевірки прийнятих від вкладника грошей» [133, с. 275–276].

Набувають поширення злочини, пов'язані з обігом пластикових платіжних засобів, які вчинюються з підробленими або викраденими платіжними засобами та їх сліпами. Технології підробки пластикових карток на сьогодні в Україні ще досить примітивні, але аналізуючи досвід іноземних країн, передові методи підробки дуже скоро можуть бути і у нас. Найбільш поширеними є протиправні посягання за допомогою сліпів (платіжних квитанцій).

Працівники торговельних пунктів, користуючись неуважністю клієнтів, роблять кілька відбитків на платіжних квитанціях, які потім використовують для оплати привласнених матеріальних цінностей.

Використання в злочинних цілях пластикових платіжних засобів передбачає виготовлення певних документів: пластикової картки, сліпів із неї, звітів матеріально відповідальних осіб, документів-посвідчень особи-пред'явника пластикових карток. Для підробки цих документів слід мати відповідну технічну базу, інструмент, сировину, фарбу, пристрої, устаткування.

Практика кримінального переслідування за такі злочини в Україні дуже незначна, і її можна охарактеризувати тільки у загальних рисах. Тут дії, пов'язані із злочинним посяганням на власність банків та їх клієнтів через комп'ютерні технології, можуть кваліфікуватися тільки за ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення»; ст. 222 «Шахрайство з фінансовими ресурсами» або ст. 194 «Умисне знищення або пошкодження майна» (якщо вважати пластикову картку майном) КК України.

Особи, що готуються до вчинення злочину, попередньо намагаються з'ясувати обставини, за яких слід буде діяти, завести знайомства з особами, що володіють необхідною інформацією.

Слід враховувати, що повноцінний ринок пластикових карток у нас в країні ще не склався, але розвивається швидкими темпами, має недостатній досвід захисту, що й використовують злочинці.

Рівень шахрайства в Україні тільки в кредитній сфері банківської діяльності в 4-5 разів перевищує світовий (найбільша кількість таких злочиніввчинюється в Києві (83%) [70, с. 165].

В Україні протягом останніх років, як і у всьому світі, у сфері надання фінансових послуг також використовується новий вид платіжних засобів – «електронні гроші» із застосуванням пластикових карток (магнітних, чіп-карт). В українських банках реалізована та діє з 1993 р. комп'ютерна система міжбанківських безготівкових платіжних розрахунків, впроваджуються й інші сучасні комп'ютерні банківські технології.

Сьогодні в обігу знаходяться 2 мільярди магнітних карт (незабаром досягне чисельності населення земної кулі). З виходом на світовий ринок країн колишнього СНД, Східної Європи і Китаю їх кількість значно зросте. Введення смарттехнологій для безготівкових розрахунків дозволить істотно підвищити рівень безпеки.

«Загальний обсяг всіх платежів, що проводяться на світовому ринку фінансовими установами за допомогою кредитних карток, за даними міжнародної статистики, складає щорічно близько 7 трильйонів доларів США. У контрасті з цією цифрою річний збиток від злочинних дій з кредитними картками в сумі близько 1,3 мільярда доларів США ледве досягає менше за половину 1% від загального грошового обороту. Незважаючи на те, що збитки, які наносяться таким видом злочину, досить мізерні порівняно із загальним об'ємом кредитних платежів, все ж їх сума вражає. Постійне її збільшення свідчить про виникнення підпільної індустрії, пов'язаної з незаконним оборотом кредитних карток» [93, с. 48].

Такі випускають дві найбільші компанії – Visa International і Master Card International. Першій належить лідерство в існуючому ринку. Цими двома компаніями лише в Канаді було випущено близько 25 млн кредитних карток. Як встановлено правоохоронними органами, з них 55475 штук використовувалися виключно обманним шляхом. [93, с. 48].

Найбільшу загрозу для системи платежів представляють злочини з підробленими пластиковими картками, використовуючи справжні номери справжніх карток. Згідно з інформацією служби безпеки фірми Master Card International, близько 90% всіх підроблених кредитних карток використовувалися організованими злочинними групами, пов'язаними з азіатськими кланами.

При підробці кредитних карток в основному використовуються номери діючих карток з великим невитраченим лімітом, «золоті» або «бізнес»-картки. Вони мають досить велику за сумою і часом мережу використання,

їх рахунки не так суворо перевіряються. Це дозволяє збільшити період часу для вчинення шахрайських дій і подовжує термін «життя» карток.

Практика свідчить, що більшість підроблених карток використовуються один раз, що робить практично неможливим простежити і викрити злочинця.

Власник картки зобов'язаний негайно повідомити в банк про будь-який випадок її втрати або викрадення. Представники служби безпеки банку збирають інформацію від продавців фірм, в яких були проведені підозрілі трансакції і повідомляють правоохоронні органи, складають детальний звіт про те, за яких умов була загублена кредитна картка.

Найбільш детально процедура проведення діяльності на ринку пластикових карток викладена в Положенні про впровадження пластикових карток міжнародних платіжних систем у розрахунках за товари, надані послуги та при видачі готівки, затвердженому правлінням НБУ 24 лютого 1997 р. № 37. Учасники ринку пластикових карток діють також згідно з законами України про валютне регулювання, про банківську діяльність, підприємництво та іншими нормативними актами, що регулюють комерційну діяльність.

Правовою основою для застосування пластикової картки є договір між емітентом картки і її держателем, що виникає у разі схвалення банком заявки клієнта на видачу йому платіжної пластикової картки і відкриття спеціального карткового рахунку (СКО).

В Україні відповідальність за вчинення злочинів з використанням пластикових платіжних засобів наступає за статтями кримінального кодексу (крадіжка, шахрайство, підробка тощо).

Подібні дії залежно від способу і фактичної належності предмета злочинних посягань можуть кваліфікуватися за такими нормами КК України:

Стаття 185. Крадіжка.

Стаття 190. Шахрайство.

Стаття 191. Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем.

Стаття 200. Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення.

Додатково дії зловмисників можуть кваліфікуватися за статтями КК: 358 – підроблення документів, печаток, штампів та бланків, їх збут, використання підроблених документів; 205 – фіктивне підприємництво; 231 – незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю; 232 – розголошення комерційної таємниці.

Проблема не в кваліфікації злочинних дій, а в тому, як їх виявити, зібрати, закріпити і використати докази.

Вченими Національної академії внутрішніх справ України узагальнено і визначено більше 12 основних способів вчинення злочинів, пов'язаних з пластиковими платіжними засобами:

«1. Операції з підробленими картками.

2. Операції з украденими/ загубленими картками.

3. Багаторазова оплата послуг і товарів.

4. Шахрайство з поштовими/ телефонними замовленнями.

5. Багаторазове зняття з рахунку.

6. Злочинні посягання з використанням підроблених, а також украдених (загублених) документів.

7. Злочинні посягання з використанням підроблених сліпів.

8. Отримання авторизації від міжнародної платіжної системи за STIP (Stand In Processing) при збоях або відсутності зв'язку.

9. Створення і використання фіктивних підприємств обслуговування за пластиковими картками.

10. Шахрайське використання банкоматів при видачі готівки.

11. Підключення електронного записуючого пристрою до POS-термінала/ банкомата («Skimming).

12. Інші види злочинних посягань.

Звертається увага на те, що класифікація видів шахрайства, запропонована вище, сформульована за функціональними ознаками і відрізняється від стандартної статистичної класифікації.

Якщо ж ґрунтуватися на міжнародній класифікації шахрайства за видами правопорушень, то картина вимальовується така:

1) шахрайство з втраченими і викраденими картками становить 72,2%;

2) шахрайство з підробленими картками – 20,5%;

3) шахрайство з картками, не отриманими законним держателем – 2,8%;

4) шахрайство з використанням рахунку – 1,4%;

5) інші форми шахрайства – 3,1%.

Коли проаналізувати співвідношення шахрайства за сервісними підприємствами, то з'ясовується, що найчастіше відбувається вчинення шахрайства через ресторани – 26,4%, готелі (мотелі) – 25%, магазини – 20,7%, бари – 10,6%, телефонні послуги – 7,4%, тобто підприємства комерційної мережі, які обслуговують пластикові картки» [71, с. 35].

Вчені, простеживши підготовку і здійснення злочинних посягань з використанням пластикових платіжних засобів, виділяють певний набір елементів, які визначають спосіб і можуть містити:

«а) знання умов придбання і використання платіжних пластикових засобів і, зокрема, тих, за допомогою яких планується вчинення крадіжок.

Вміння шахрая триматися впевнено, виглядати зовні так само, як більшість клієнтів, тобто «ввійти в роль», щоб не викликати підозри обслуговуючого персоналу і не стати об'єктом їх пильної і підвищеної уваги;

б) наявність (залежно від способу посягань):

– справжньої пластикової (кредитної або дебетової) картки;

– бланків рахунків (сліпів);

– даних держателів і номерів банківських рахунків, які планується використовувати при вчиненні злочинного посягання;

– матеріалів для виготовлення повністю або частково підроблених пластикових карток;

– обладнання для виготовлення таких карток;

– обладнання для рекодування і знищення первинної інформації на магнітній стрічці з метою зміни номера картки і терміну її дії. При цьому зміст лицьового боку картки може не збігатися з інформацією на магнітній стрічці (для цього використовуються викрадені реальні картки з голограмою та іншими засобами захисту із реальною інформацією, взятою з іншої картки);

– спільників у сервісних точках обслуговування;

– спільників у банках-емітентах пластикових карток або серед розробників систем захисту;

– спільників на пошті для викрадення карток, які пересилаються поштою, або одержання від них інформації з метою забезпечення шахрайських дій;

в) зв'язки:

– з особами, які збувають викрадені картки;

– з персоналом сервісних точок, де приймаються до обслуговування ті або інші пластикові платіжні засоби;

г) навички підробки підпису на рахунку або роздруковці касового термінала від імені іншої особи відповідно до зразка, який є на картці;

д) наявність документів на ім'я держателя картки» [71, с. 56].

Підроблені пластикові картки виготовляються з використанням подібних методів друку, а іноді й тих самих засобів захисту, які використовуються для справжніх кредитних карток.

Організовані злочинні групи спроможні повністю підробити пластикові картки, послідовно провадять збір інформації про реальний рахунок у банку (ці дані можуть бути отримані навіть із копії рахунків за товари, знайденої випадково) або картку з великим кредитом; доставку чистих пластикових заготовок; формують (ембосують) на заготовці рельєфне зображення номера реального рахунку; реалізують картки в торгові чи сервісні точки і отримують товар чи послуги.

Кредити за такими картками, як правило, використовуються одночасно і повністю, після чого картка знищується.

Викрадені пластикові картки в одній країні, можуть бути використані в іншій.

«Класифікація суб'єктів шахрайства з використанням пластикових платіжних засобів може бути розглянута за такою схемою:

– персонал обслуговуючих сервісних точок;
– особи, котрі займаються викраденням карток;
– особи, які використовують загублені картки;
– банківські службовці;
– особи, які виготовляють підроблені пластикові картки;
– особи, що є законними держателями пластикових карток» [116, с. 65].

При розслідуванні злочинних посягань з використанням кредитних карток необхідна документація отримується з таких джерел: законний власник картки; продавець, який проводив трансакцію; фірма, що випустила картку; поштові установи; транспорті компанії; обвинувачений.

Важливо налагодити ефективну взаємодію між правоохоронними органами і службами безпеки платіжних систем для запобігання, своєчасного виявлення, розкриття і розслідування злочинів, пов'язаних з використанням пластикових платіжних засобів.

Цілком справедливо акцентується увага на тому, що «для правоохоронних органів потреба у взаємодії зумовлюється такими об'єктивними чинниками:

1) служба безпеки платіжних систем цілеспрямовано, послідовно і професійно виконує роботу щодо запобігання втрат від злочинних посягань;

2) служба безпеки постійно вживає заходів, пов'язаних з технічною захищеністю як самих пластикових карт, так і комунікацій банківських мереж;

3) служба безпеки постійно вживає заходів щодо запобігання витоку інформації з підрозділів по роботі з пластиковими картками. Основним принципом є чітке розмежування службових обов'язків співробітників і відповідно до цього обмеження доступу до конфіденційної інформації до мінімуму, потрібного для роботи. Ці заходи знижують ризик і можливість вступу у зговір злочинців зі службовцями;

4) платіжні системи регулярно поширюють бюлетені безпеки, в яких публікують службовий матеріал і статистику про злочини з картками, повідомляють прикмети злочинців і ознаки підроблених карток, які надійшли в незаконний обіг;

5) серед профілактичних заходів служби безпеки важливе місце посідає робота з клієнтами, спрямована на підвищення культурного рівня користування «пластиковими грішми».

Для служб безпеки банків потреба у взаємодії з правоохоронними органами зумовлюється головним чином тим фактом, що за українським законодавством ніякі приватні служби безпеки не мають права вживати певних заходів на підставі вчиненого злочину. Це право за законом мають тільки правоохоронні органи» [71, с. 65].

Взаємодія між правоохоронними органами і службами безпеки платіжних систем повинна провадити за такими основними напрямами: своєчасне виявлення передумов і фактів злочинних посягань на використання пластикових платіжних засобів не за призначенням. Ефективне реагування на виявлені факти злочинних посягань. Оперативне отримання потрібної інформації в міжнародних платіжних системах. Обмін інформацією, зокрема ведення спільних обліків. Взаємна допомога у збиранні доказів за фактами правопорушень. Вживання загальних профілактичних заходів. Аналітична робота, обмін досвідом.

«Найкраще взаємодія і співпраця правоохоронних органів і служб безпеки платіжних систем побудована в тих країнах, де їх взаємні зобов'язання максимально формалізовані на законодавчому рівні. Така практика притаманна більшості розвинутих країн, в яких картковий бізнес контролює величезні фінансові потоки і є складовою повсякденного життя. Інший варіант організації взаємодії, наприклад у Росії, передбачає визначення взаємних зобов'язань на договірній основі» [71, с. 66].

В Україні представниками служб безпеки платіжних систем є спеціалізовані служби безпеки банків і процесингових компаній.

Надійним механізмом попередження і профілактики злочинних посягань з використанням пластикових платіжних засобів є побудова і реалізація комплексної, багатофункціональної системи безпеки пластикових платіжних засобів.

На початку 2004 р. в Одесі було затримано трьох молодих місцевих жителів при намаганні незаконно зняти через банкомат велику суму грошей з допомогою підроблених пластикових карток. Використовуючи доступ до картрахунків одного із зарубіжних банків, зловмисники неодноразово знімали із рахунків клієнтів великі суми грошей, викравши таким чином 0,5 млн доларів США. За один раз «взломщики» знімали із рахунків своїх жертв від 10 до 40 тис. доларів. За фактом шахрайства порушено кримінальну справу. Про широкі масштаби злочинної індустрії свідчить той факт, що в процесі проведених обшуків у підозрюваних вилучено 61 підроблену картку, 135 заготовок до них, прилад для нанесення інформації на магнітні смуги пластикових карток.

Співробітники правоохоронних органів прогнозують подальше зростання кількості злочинів в Україні з використанням пластикових карток. Підтвердженням цьому є той факт, що вітчизняні злочинці уже

налагоджують канали надходження в Україну із-за кордону втрачених чи викрадених карток [177].

Основними причинами, які сприяють вчиненню шахрайства з використанням пластикових платіжних засобів є: нерозумна економія на засобах захисту пластикових платіжних засобів; невчасне і не всеохоплююче використання «стоп-листів» з метою припинення шахрайства з картками.

Передумовою злочинних посягань є недостатня взаємодія банківських структур і правоохоронних органів, про що свідчить такий приклад.

Як повідомила газета «Факти» ще 7 квітня 1998 р. у Вінницьке регіональне управління Промінвестбанку влаштувався на роботу студент 5 курсу місцевого державного технічного університету С.Соляниченко. Він, маючи добру технічну підготовку, швидко розібрався у багатьох тонкостях банківської справи, зокрема в операціях, пов'язаних з рухом безготівкових коштів. Підібрав помічників із числа мешканців м.Львова, і дізнався особистий пароль одного із банківських співробітників, щоб через нього увійти в електронну базу даних. Відкривши розрахункові рахунки у Львівському відділенні Акціонерно-комерційного банку «Галицький» і Львівському відділенні Ощадбанку, Соляниченко скритно увійшов в центральну базу даних і зняв з рахунку одного із підприємств кілька тисяч гривень. Поділивши всю суму порівну між співучасниками, перевів їх на львівські рахунки, відкриті за фальшивими документами.

Комп'ютерна програма спрацювала надійно, файли знищити зловмиснику не вдалося. Паралельно включилися резервні захисті функції програми, які зупинили і заблокували рух засобів по всьому регіональному управлінню Промінвестбанку.

Завдяки оперативному виявленню переводу–кражі внутрішньою службою безпеки банку, а також своєчасному і компетентному втручанню УСБУ Вінницької і Львівської областей, було порушено кримінальну справу і не допущено виконання злочинного наміру.

Аналогічний випадок, але з іншими результатами, мав місце в Туркменії. Він увінчався успіхом, в результаті чого викрадено 41 млн доларів, про що повідомила газета «Сегодня» 3 жовтня 2002 р. Ця сума частинами зникла з рахунку Центробанку Туркменістану в німецькому Deutsche Bank, яким особисто користувався туркменський президент С. Ніязов. До цієї події причетний співробітник туркменського банку Арслан Какаєв, який встиг за кілька днів до виявлення зникнення грошей поміняти місце проживання. Він перевів гроші із рахунку Deutsche Bank на рахунки компаній в офшорних зонах та в Росії.

Здійснились, і не вперше, слова «хрещеного батька» одного із сімейств американської мафії Дон Віто Карлеоне: «чиновник з портфелем вкраде набагато більше, ніж тисяча гангстерів, озброєних автоматами».

Халатне ставлення окремих службовців банку до збереження службової інформації або недбале збереження пластикових платіжних засобів, умисне співробітництво банківських службовців із злочинцями сприяє злочинним посяганням з використанням пластикових карток. І ще те, що бланки, які використовують для оформлення сліпів, не в усіх банках є бланками суворої звітності, що полегшує доступ до них шахраям.

При прийомі пластикових карток до оплати слід перевірити їх відповідність встановленій формі за всіма параметрами згідно з інструкцією. При огляді пластикової картки, що викликає сумнів, доцільно порівняти її зі справжньою карткою.

Кардинально ускладнюють завдання, що стоять перед шахраями, чіпові картки, оснащені мікросхемою. Копіювання чіпової картки практично неможливе, враховуючи високу технологічність процесу її виготовлення. Розробники тримають прилади виготовлення кристалу в великому секреті.

До аналогічних заходів можна віднести використання прихованих ключів-паролів. Коли зловмисник будь-яким чином одержав доступ до електронного терміналу, то, маючи інформацію про чужий рахунок, спробує ним скористатися. Але його дії можуть бути, як ми переконалися раніше, заблоковані, оскільки кожна ланка ланцюжка, по якому проходить трансакція, захищена ключами.

Привабливою для злочинців роблять банківську систему глобальність, простота і зручність користування мережею Internet.

Перший у світі банк (Security First Network Bank) провадить трансакції через мережу Internet. Клієнтам банку надається можливість провести фінансові операції через глобальні мережі та Internet. Масовий перехід на сучасні технології стримується проблемою забезпечення інформаційної безпеки в цій глобальній мережі.

Відкритість і незахищеність банку, інформаційна система якого пов'язана з Internet, значно вища, ніж комутуючі лінії, які приходять на модемний пул банківського вузла зв'язку.

Застосування мережі Internet вимагає забезпечення компонентів банківської безпеки. Мережа Internet є відкритою структурою без спеціальних елементів безпеки. Проте правильно поставлена система безпеки, що включає належну програмно-апаратну підтримку і застосування сучасних криптографічних методів захисту інформації, що здатна забезпечити надійне функціонування сучасних фінансових технологій у рамках глобальної міжнародної інформаційної мережі Internet.

Як свідчить практика, головну загрозу становить некомпетентність системних адміністраторів: 90% систем використовують тільки 10% можливостей захисту. Окремим питанням слід виділити безпеки Web-технологій і відсутність для них політики безпеки [70, с. 178].

Для банків при використанні мережі Internet є небезпека, пов'язана з так званими макровірусами, що уражають файли документів і електронні таблиці. Із збільшенням електронного обігу документів по глобальній мережі ця небезпека буде усе більш реальною для банків.

Перед ними постає проблема: з одного боку, мережа Internet – безсумнівно, величезний потенційний ринок для банківських послуг, але з іншого – запровадження цієї мережі викликає потребу розробки надійних засобів безпеки (технічного боку проблеми ми не будемо торкатись, оскільки вона детально розглянута в низці праць) [93, 70].

Істотною проблемою використання сучасної мережі Internet є слабкий правовий захист від комп'ютерних злочинів. На жаль, до цих пір Internet не є суб'єктом або об'єктом права. Це ускладнює правове обгрунтування позовів за злочинами, вчиненими через Internet. Часто злочини через Internet вчинюються із-за кордону, тобто поза вітчизняним правовим полем.

Підтвердженням цьому може слугувати одна з кримінальних справ, розслідування якої провадилося російськими правоохоронними органами у тісному контакті з ФБР США. Кримінальна справа була порушена у відношенні громадян Російської Федерації, які вчинили викрадення грошових коштів у великих розмірах із «City Bank of Amerika», розташованого в Нью-Йорку. Злочинна група діяла в Санкт-Петербурзі з червня до вересня 1994 р., використовуючи електронну комп'ютерну мережу Internet, подолавши при цьому декілька рубежів захисту від несанкціонованого доступу. В результаті злочинцями було здійснено близько 40 переказів грошових коштів на загальну суму 10 млн 700 тис. 952 дол. США з рахунків клієнтів банку на рахунки осіб, що входили до складу злочинної групи і проживали у шести країнах світу: США, Великої Британії, Ізраїлі, Швейцарії, ФРН та Росії. Коли один із злочинців вилетів на запрошення родичів у Лондон, він був заарештований правоохоронними органами Великої Британії. Лондонський суд, який відбувся в серпні 1995 р. відклав прийняття рішення у цій справі на невизначений термін, оскільки в ході судового розгляду за допомогою адвоката було доведено, що для отримання доступу до рахунків клієнтів «Сітібанку» підсудний використав як знаряддя вчинення злочину комп'ютер, який знаходився на території Росії, а не на території США, як вимагає того кримінальне законодавство Великої Британії. З огляду на зазначене вище, прохання американських та російських представників про видачу їм заарештованого було судом відхилено. Внаслідок правоохоронні органи США і Росії були позбавлені можливості завершити роботу з розкриття низки злочинів, вчинених членами вказаної злочинної групи і заарештованих в цих країнах [70, с.179–180].

У банківській діяльності за потреби компетентними органами може проводитися вилучення із банків як електронних носіїв інформації, так і документів. Але як свідчить практика, банками не завжди робляться завірені копії таких документів. Тому ми детально зупинимося на цій процедурі.

Відповідно до ст.12 закону «Про організаційно-правові основи боротьби з організованою злочинністю» спеціальні підрозділи з боротьби з організованою злочинністю МВС і СБ України за постановою та санкцією відповідного прокурора з нагляду за виконанням законів спеціальними підрозділами з боротьби з організованою злочинністю, а у невідкладних випадках – з наступним повідомленням прокурора впродовж доби, в разі загрози знищення, приховування або втрати предметів чи документів, які можуть бути використані в розкритті та розслідуванні злочинної діяльності, мають право вилучати предмети і документи із складанням відповідного акта. Копії акта вручаються представникові банківської установи, як правило, – її керівникові.

Про проведення виїмки особа, яка її провадить, складає протокол у двох примірниках з дотриманням правил ст.85 КПК. У протоколі зазначають: підстави для виїмки; приміщення чи інше місце, в якому її було проведено; особу, в якої проведено вилучення; дії особи, яка проводить виїмку і результати виїмки. Стосовно кожного предмета, що підлягає вилученню, має бути зазначено, в якому саме місці й за яких обставин він був вилучений.

Виїмка проводиться на підставах та в порядку, визначених гл. 16 КПК, за постановою слідчого.

Усі документи і предмети, що підлягають вилученню, мають бути пред'явлені понятим та іншим присутнім особам і перелічені в протоколі вилучення чи в доданому до нього описі із зазначенням їхньої назви, кількості, міри, ваги, матеріалу, з якого вони виготовлені, та індивідуальних ознак.

Під час вилучення оригіналу або копії документа рекомендується зробити про це відповідний запис у протоколі виїмки.

Відповідно до п. 2.1.1. «Положення про організацію бухгалтерського обліку та звітності в банківських установах України», що затверджена постановою правління НБУ від 30 грудня 1998 р. № 566 (зареєстрована в Мін'юсті 1 лютого 1999 р .за № 56/3349), в присутності представників правоохоронних органів, які провадять виїмку, відповідним службовим особам банку рекомендується зняти копії з оригіналів документів та скласти реєстр цих документів із зазначенням підстав і дати їхнього вилучення й завірити її у відповідальних осіб банків і представників правоохоронних органів.

Під час вилучення копії документа, оригінал якого містить інформацію на електронних носіях (зокрема, в разі перенесення такої інформації на паперові носії), копію цього документа (листом НБУ від 24 жовтня 2000 р. № 43-311/4502-7137) рекомендується завірити керівником банківської установи, головним бухгалтером та особою, яка провела виїмку, й зробити про це відповідний запис у протоколі. У разі вилучення електронних носіїв інформації рекомендується потрібну для роботи інформацію зняти на інші електронні носії інформації.

Нормативно-правове регулювання використання електронних носіїв інформації в банківській системі провадиться на основі прийнятих у 2003 р. законів України «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», а також відповідно до постанов Правління Національного банку України від 18 червня 2003 р. № 254 «Про затвердження Положення про організацію операційної діяльності в банках України», від 10 червня 1999 р. № 280 «Про затвердження правил організації захисту електронних банківських документів» (із змінами, внесеними згідно з № 495 від 4 грудня 2001 р.), від 8 липня 1998 р. № 267 «Про порядок і передачі інформації від установ банків до органів державної податкової служби електронними засобами» [додаток В.23, с. 92–95].

Зокрема, зазначеними постановами Нацбанку передбачається, що програмне забезпечення банку має відповідати таким вимогам інформаційної безпеки:

– наявність системи захисту інформації, яку не можна відключити і неможливо провести оброблення інформації без її використання;

– забезпечення належного захисту інформації під час її передавання між різними підсистемами формування та оброблення інформації;

– для автоматизованих систем, які функціонують у режимі «клієнт-сервер», доступ користувачів до бази даних має відбуватися лише через додаткове програмне забезпечення, за допомогою якого провадиться автентифікація осіб, яким дозволено користуватися цією базою даних;

– автентифікація користувача на кожному робочому місці та під час виконання будь-яких операцій;

– забезпечення блокування роботи на кожному робочому місці під час багаторазових спроб (не більше трьох) неправильного введення паролю, якщо використовується парольний захист;

– наявність безперервного технологічного контролю за цілісністю інформації та накладання/перевірка цифрового підпису на всіх банківських документах на всіх етапах їх оброблення;

– передавання електронних банківських документів, втрата або несанкціоноване ознайомлення з якими може завдати збитків банку, його установі або клієнту банку, відповідними каналами зв'язку, електронною

поштою або в режимі on-line лише зашифрованими з обов'язковим наданням підтвердження про їх отримання;

– обов'язкова реєстрація всіх спроб доступу, усіх операцій та інших дій, їх фіксація в автоматизованій системі в захищеному від модифікації електронному журналі з постійним контролем його цілісності.

Крім того, банкам слід:

– суворо дотримуватися і перевіряти виконання вимог щодо технічного та технологічного забезпечення їх діяльності, зокрема розміщення програмно-апаратних комплексів на таких комп'ютерах, що мають забезпечити їх надійне функціонування;

– вживати заходів для забезпечення безперебійного електроживлення та наявності резервних каналів зв'язку;

– перевіряти виконання вимог щодо організації захисту інформації в програмно-технічних комплексах згідно з нормативно-правовими актами Національного банку та вимогами розробників систем захисту інформації.

Національний банк України, комерційні банки та їх установи зобов'язані:

– надавати інформацію в електронному вигляді засобами електронної пошти НБУ на адресу державних податкових адміністрацій (далі – ДПА) в Автономній Республіці Крим, областях, містах Києві та Севастополі з використанням засобів захисту Національного банку України;

– забезпечити контроль ідентифікаційного коду платника на розрахунковому документі, в якому один із рахунків бюджетний, на відповідність коду клієнта в електронному реєстрі клієнтів банку та формування програмним забезпеченням банку інформації.

Відповідальність за зберігання та нерозголошення конфіденційної банківської інформації в обчислювальних мережах ДПА покладається на податкові органи згідно з чинним законодавством.

Постановою № 280-1999 р. затверджено Правила організації захисту електронних банківських документів в установах, включених до інформаційно-обчислювальної мережі Національного банку України та Правила організації захисту електронних банківських документів в установах Національного банку України (тільки до служб захисту установ НБУ).

Система захисту електронних банківських документів (СЗЕБК) в інформаційно-обчислювальній мережі НБУ побудована згідно з додатком 6 до Положення про міжбанківські розрахунки в Україні і складається з комплексу апаратно-програмних засобів криптографічного захисту та ключової системи до них, технологічних і організаційних заходів щодо захисту інформації в інформаційно-обчислювальній мережі НБУ.

СЗЕБК охоплює всі етапи розробки, впровадження та експлуатації програмно-технічного забезпечення інформаційно-обчислювальної

мережі та включає чіткий розподіл відповідальності на кожному етапі підготовки, обробки та виконання електронних банківських документів на всіх рівнях. Вона є єдиною для усіх інформаційних задач НБУ і СЕП. Для підвищення ступеня захисту електронних розрахункових документів у СЕП використовуються додаткові засоби, включаючи бухгалтерський контроль. Технологічні та криптографічні засоби безпеки використовуються не тільки в СЕП, а й у всіх інформаційних задачах НБУ. Для забезпечення контролю за виконанням вимог щодо захисту інформації у банківських установах, що є учасниками інформаційно-обчислювальної мережі НБУ, служби захисту інформації регіональних управлінь НБУ мають виконувати планові (а в разі потреби – і позапланові) перевірки всіх установ, що використовують засоби захисту інформації НБУ.

Забороняється передавати, навіть тимчасово, засоби захисту іншим установам або особам, у тому числі й іншим установам однієї юридичної особи.

Відповідальність за виконання вимог режимних умов до приміщень покладається на керівництво банківських установ.

Побудова ключової системи виконується службою захисту інформації НБУ згідно з діючою системою захисту. Ключова система вміщує ключі асиметричного шифрування, що генеруються в банківських установах за допомогою наданих генераторів-ключів, та ключі симетричного шифрування, що використовуються для апаратного шифрування.

Забороняється використання засобів захисту НБУ у внутрішніх платіжних системах банків, системах «клієнт-банк» та інших програмних комплексах, які знаходяться за межами системи автоматизації банку.

Усі питання, пов'язані з організацією безпеки електронних платежів у СЕП НБУ та інформаційних системах НБУ, вирішуються через службу захисту інформації того регіонального управління НБУ, з яким укладений договір про використання криптографічних засобів захисту інформації в інформаційно-обчислювальній мережі НБУ.

Електронна картка для банківських установ, що розташовані за межами обласного центру, надсилається спецзв'язком у подвійному конверті або передається через відповідальну особу банківської установи. Для банківських установ, що розташовані в обласному центрі, картка передається через відповідальну особу банківської установи.

Зберігається електронна картка в неробочий час або в робочий час, якщо вона не використовується в роботі, у сейфі адміністратора АРМ-НБУ.

Після завершення робочого циклу використання (дата призначається управлінням захисту інформації НБУ) електронна картка у дводенний строк разом із супровідним листом банківської установи повертається до служби захисту інформації регіонального управління НБУ.

У разі виходу з ладу електронної картки до завершення робочого циклу використання слід: виконати дії для забезпечення переходу на резервне програмне шифрування; поінформувати електронною поштою службу захисту інформації регіонального управління НБУ про вихід з ладу електронної картки; повернути встановленим порядком (нарочним або спецзв'язком) до служби захисту інформації регіонального управління НБУ зіпсовану електронну картку разом із супровідним листом, один примірник якого залишається в службі захисту інформації регіонального управління НБУ, другий зберігається в банківській установі. Після отримання нової електронної картки і нового комплекту таблиць KMEP.BIN, TABLE.BIN вживаються заходи для переходу до використання апаратних засобів шифрування. У разі навмисного або ненавмисного пошкодження або втрати електронної картки потрібно провести службове розслідування, копії матеріалів якого подати до служби захисту інформації регіонального управління НБУ. При цьому слід відшкодувати збитки від пошкодження електронної картки відповідно до договірних зобов'язань.

Призначення відповідальних за роботу із засобами криптозахисту і звільнення їх від цих обов'язків належить до компетенції керівництва банківської установи.

Банківська установа зобов'язана негайно (по телефону) інформувати службу захисту інформації регіонального управління НБУ у таких випадках: виконання (спроби виконання) фіктивного платіжного документа; компрометації засобів криптозахисту; пошкодження засобів криптозахисту; несанкціоноване проникнення в приміщення АРМ-НБУ (пошкодження вхідних дверей, грат на вікнах, спрацювання сигналізації при нез'ясованих обставинах тощо); проведення правоохоронними органами та іншими державними установами перевірки комерційної діяльності банківської установи, якщо при цьому виникають умови для компрометації діючих засобів криптозахисту; виникнення інших аварійних або надзвичайних ситуацій, що створюють реальні передумови до розкрадання, втрати, пошкодження тощо засобів криптозахисту.

Безпосередньо контроль за станом захисту електронної банківської інформації в банківській установі провадить адміністратор захисту інформації. Цей контроль провадиться як у процесі повсякденної діяльності, виходячи із ситуації, що конкретно складається на тій або іншій дільниці роботи, так і в разі планових перевірок.

Контроль за станом захисту електронних банківських документів покладений на службу захисту інформації регіонального управління НБУ. Контроль провадиться в процесі перевірок, які виконує співробітник (співробітники) служби захисту інформації регіонального управління НБУ.

Окрему проблему становить банківська таємниця та її захист.

3.6. Банківська таємниця та її захист

У процесі фінансової діяльності банки оперують різною інформацією, класифікація якої подана у додатку Б.4. Половину її становить інформація з обмеженим доступом, яка поділяється на конфіденційну і таємну, а остання – на банківську таємницю і комерційну (додаток Б. 5).

Відповідно до чинного законодавства банківська інформація, операції, рахунки та вклади клієнтів і кореспондентів, знаходяться в Україні під охороною.

Найбільш регламентованим феноменом банківської діяльності, який разом з тим став предметом постійної уваги, є банківська таємниця.

Визначення банківської таємниці дає ст. 52 Закону України «Про банки і банківську діяльність». Згідно з нею до банківської таємниці належать відомості про операції, рахунки та вклади клієнтів і кореспондентів банку. Це друге, поряд з державною таємницею, однозначне визначення таємниці на законодавчому рівні. Не дозволяється обмежувати чи, навпаки, розширювати відомості, що становлять банківську таємницю. Окрім цього, поняття комерційної таємниці подається у ст. 30 Закону України «Про підприємства в Україні», але не так конкретно. Тут зазначено, які відомості можуть бути віднесені до комерційної таємниці (відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами, іншою діяльністю підприємства, розголошення яких може завдати шкоди інтересам підприємства). Однією з умов віднесення відомостей до комерційної таємниці є те, що вони не повинні бути державною таємницею. Стаття 1 цього Закону визначає: «Підприємство – самостійний господарюючий статутний суб'єкт, який має права юридичної особи та здійснює виробничу, науково-дослідницьку і комерційну діяльність з метою одержання відповідного прибутку». Згідно з цим визначення, до підприємств можуть бути віднесені й комерційні банки, які теж можуть мати право на комерційну таємницю.

Поняття «конфіденційної інформації» наведено в Законі України «Про інформацію», де зазначено, що остання за своїм правовим режимом є інформацією з обмеженим доступом і її становлять «... відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов» (ст. 30).

За визначенням Юридичної енциклопедії: «Банківська таємниця – інформація про операції, рахунки та вклади клієнтів і кореспондентів банку

із спецрежимом використання. Носії такої інформації мають гриф таємності, оскільки вона є різновидом службової таємниці. Порядок користування відповідними відомостями регулюється Законом України «Про банки і банківську діяльність» та ін. законодавчими актами. Банківська таємниця охороняється законом, усі службовці банків зобов'язані її зберігати. У передбачених законодавством випадках довідки про банківські операції, рахунки та вклади видаються за письмовою вимогою відповідних державних органів (суду, прокуратури, органів внутрішніх справ, служби безпеки), а також аудиторським організаціям. Довідки щодо рахунків і внесків у разі смерті їх власників видаються особам, які вказані в заповіті, державним нотаріальним конторам з приводу справ успадкування, іноземним консульським установам. Розголошення банківської таємниці є підставою для притягнення винних осіб до юридичної відповідальності» [173, с. 190–191].

Дещо уточнюючи визначення цього феномену , доповнюючи наведене, дала Банківська енциклопедія: банківська таємниця – відомості, що не підлягають розголошенню. До них належать відомості про стан рахунків клієнтів та виконуваних операцій. Такі відомості можуть надаватись самим клієнтам, судовим, слідчим та фінансовим органам. Банківська таємниця є різновидом комерційної таємниці, яка полягає в тому, що фірми і банки приховують одне від одного відомості про операції з метою одержання вищих прибутків. Публікація балансів не виключає банківської таємниці, оскільки відомості звичайно даються взагалі, не розкриваючи конкретних операцій банків, їх зв'язків з клієнтурою [63, с. 22].

Отже, на наш погляд, в сконцентрованому вигляді **банківська таємниця** – це відомості, що не підлягають розголошенню і охороняються державою як службова таємниця. До них належить визначений законом перелік відомостей про стан рахунків клієнтів, виконуваних операцій тощо. Банківська таємниця хоча і не відноситься до державної таємниці, є різновидом комерційної таємниці, яка забезпечує одержання найвищих прибутків.

Розмежовуючи поняття банківської та комерційної таємниць, конфіденційної інформації, законодавець встановлює і різний правовий режим захисту такої інформації.

Перелік відомостей, які складають банківську таємницю, встановлюється законом «Про банки і банківську діяльність», що свідчить про значущість інформації, яка належить до банківської таємниці. Ст. 60 цього закону так характеризує банківську таємницю: «Інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту, є банківською таємницею».

Таким чином, банківською таємницею є:

– відомості про стан рахунків клієнтів, у тому числі стан кореспондентських рахунків банків у Національному банку України;

– операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;

– фінансово-економічний стан клієнтів;

– системи охорони банку та клієнтів;

– інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності;

– відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

– інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

– коди, що використовуються банками для захисту інформації. Інформація про банки чи клієнтів, яка збирається під час проведення банківського нагляду, становить банківську таємницю.

Правовий режим захисту банківської таємниці встановлено Законом України «Про банки і банківську діяльність».

Згідно зі ст. 60 закону інформація щодо діяльності та фінансового становища клієнта, яка стала відома банку в процесі обслуговування клієнта і взаємовідносин з ним або третіми особами при наданні послуг банку і розголошування якої може завдати матеріальної або моральної шкоди клієнту, становить банківську таємницю.

До банківської таємниці належать і відомості про стан рахунків клієнтів, у тому числі стан кореспондентських рахунків у Національному банку.

Стаття 61 закону зобов'язує банки забезпечити зберігання банківської таємниці.

Службовці банку при вступі на посаду підписують зобов'язання стосовно зберігання банківської таємниці. Вони зобов'язані не розголошувати і не використовувати з вигодою для себе або для третіх осіб конфіденційну інформацію, яка стала їм відома при виконанні своїх службових обов'язків.

Порядок розкриття банківської таємниці регламентується ст. 62 закону, яка передбачає, що інформація стосовно юридичних і фізичних осіб, яка містить банківську таємницю, розкривається банками:

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

2) на письмову вимогу суду або за рішенням суду;

3) органам прокуратури, Служби безпеки, Міністерства внутрішніх справ на їхню письмову вимогу стосовно операцій за рахунками конкретної

юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу;

4) органам Державної податкової служби на їхню 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.

У цій же статті зазначено, що вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, повинна:

– бути викладена на бланку державного органу встановленої форми;

– бути надана за підписом керівника державного органу (або його заступника) і скріплена гербовим друком;

– містити передбачені цим законом підстави для отримання цієї інформації;

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

Довідки щодо рахунків (внесків) у разі смерті їх власників надаються банком особам, вказаним власником рахунку (внеску) в заповітному розпорядженні банку, державним нотаріальним конторам або приватним нотаріусам, іноземним консульським установам у справах спадщини за рахунками (внесками) померлих власників рахунків (внесків).

Банку забороняється надавати інформацію про клієнтів іншого банку.

Обмеження щодо отримання інформації, яка містить банківську таємницю, передбачені цієї статтею, не поширюються на службовців Національного банку або уповноважених ними осіб, які в межах повноважень, наданих законом «Про Національний банк України», виконують функції банківського нагляду або валютного контролю.

Національний банк у своєму листі від 19 квітня 2001 р. № 18-112/1467-2599 дав роз'яснення з деяких питань виконання закону.

Так, дозвіл на розкриття банком інформації, що містить банківську таємницю, який дається юридичною особою, має бути підписаний керівником або уповноваженою ним особою і скріплений гербовою печаткою юридичної особи, а дозвіл на розкриття банком цього роду інформації, наданий фізичною особою, підписується цією особою, і її підпис має бути завірений керівником банку або уповноваженою ним особою і скріплений печаткою банку або завірений нотаріально.

Крім того, в листі роз'яснюється, що в запитах має чітко вказуватися календарний проміжок часу, за який слід надати інформацію щодо операцій за рахунками.

Інакше встановлено правовий режим захисту комерційної таємниці. Згідно з ч. 2 ст. 30 Закону України «Про підприємства в Україні» порядок захисту відомостей, що становлять комерційну таємницю визначає

керівник підприємства (банку). Цією самою статтею надається право керівникові визначати склад і обсяг таких відомостей.

Аналогічним чином визначений і правовий режим захисту конфіденційної інформації. Відповідно до ч. 3 ст. 30 Закону України «Про інформацію» власникам конфіденційної інформації надано право самим включати її до категорії конфіденційної, визначати режим доступу до неї та встановлювати систему (способи) її захисту.

Намагання у 2003 р. спростити доступ до банківської таємниці зразу ж викликали заперечення у ЗМІ. Газети засяяли заголовками на кшталт: «Віднині банківської таємниці в Україні немає» («Факти«, 13 березня 2003 р.) або «Банківську таємницю хочуть зробити явною» («Деловая столица», 17 березня 2003 р.). Підставою для таких висновків в першому випадку стало роз'яснення Конституційного суду України щодо наявності права у народних депутатів направляти депутатські запити і одержувати інформацію, яка є банківською таємницею, а також інформації про провадження наглядових дій і вживання заходів впливу до банків і осіб, охоплених наглядовою діяльністю НБУ, якщо такий запит пов'язаний з їхньою депутатською діяльністю.

Заперечення виникли у зв'язку з тим, що ні народні депутати, ні парламентські комітети, ні тимчасові слідчі депутатські комісії в перелік органів, яким може бути надана така інформація згідно зі ст. 62 Закону України «Порядок розкриття банківської таємниці» Закону України «Про банки і банківську діяльність», не входять.

Конституційний суд України своїм рішенням від 5 березня 2003 р. № 5-рп/2003 у справі за конституційним поданням Національного банку України про офіційне тлумачення положень ст. 86, ч. 2 ст. 89 Конституції України, ч. 2 ст. 15, ч. 1 ст. 16 Закону України «Про статус народного депутата України» (справа про звернення народних депутатів України до Національного банку України) визнав, що народний депутат має право на сесії Верховної Ради України звернутися із запитом до Голови Національного банку України про надання інформації, яка становить банківську таємницю, а також про провадження наглядових дій та застосування заходів впливу до банків та осіб, які охоплюються наглядовою діяльністю Національного банку України.

Голова Національного банку України, розглядаючи запит, зобов'язаний повідомити народного депутата України про результати розгляду, тобто дати офіційну відповідь.

Народний депутат України має право звернутися до Національного банку України або його посадових осіб з письмовою пропозицією (депутатським зверненням) про надання інформації, яка становить банківську таємницю, а також про провадження наглядових дій та

вживання заходів впливу до банків та осіб, які охоплюються наглядовою діяльністю Національного банку України, якщо це пов'язано з депутатською діяльністю.

Голова Національного банку України або інші посадові особи Національного банку України, розглядаючи звернення, мають повідомити народного депутата про результати розгляду.

Комітет Верховної Ради України має право звернутися до Національного банку України або його посадових осіб з приводу надання інформації, яка становить банківську таємницю, а також провадження наглядових дій, застосування заходів впливу до банків та осіб, які охоплюються наглядовою діяльністю Національного банку України, якщо це пов'язано із законопроектною роботою, підготовкою і попереднім розглядом питань, віднесених до повноважень Верховної Ради України.

Голова Національного банку України або інші посадові особи Національного банку України мають повідомити комітет Верховної Ради України про результати розгляду.

Зазначені джерела преси наполягали на своєму, що така інформація депутатам може бути видана лише із згоди клієнта, стосовно якого запитується. Або, як радить «ДС» – через нещодавно створену при Мінфіні фінансову розвідку, що буде вирішувати якою інформацією ділитися з фіскальними чи правоохоронними органами. Як висловився з цього приводу 17 березня 2003 р. Голова Нацбанку С.Тігіпко кореспонденту «ДС»: На грошові засоби та інші цінності юридичних осіб і громадян, розміщені в банках, арешт може бути накладено тільки за рішенням судів і постановами слідчих органів або арбітражних судів у випадках, передбачених законодавством.

Аналіз нормативно-правового регулювання банківської та комерційної таємниці свідчить про таке. Потреба у збереженні та захистові комерційної таємниці було проголошено вперше в Україні Законом України «Про підприємства в Україні» від 27 березня 1991 р. Пізніше, 7 червня 1996 р. Законом України «Про захист від недобросовісної конкуренції» неправомірне збирання, розголошення та використання комерційної таємниці без згоди на те уповноваженої особи було кваліфіковано як одна із форм недобросовісної конкуренції (ст. 1 гл. 4).

Усі відомості, якими так чи інакше може володіти банк, поділяються на три види: 1) відомості, які становлять державну таємницю; 2) відомості, які в силу вказівки законодавства не становлять комерційної таємниці і 3) відомості, які можуть складати комерційну таємницю.

Співвідношення державної та банківської таємниці, на наш погляд, полягає ось в чому. Комерційна таємниця не відноситься до відомостей, які становлять державну таємницю. На відміну від комерційної таємниці,

режим секретності державної таємниці встановлюється виключно законами і підзаконними актами України. Наприклад, питання доступу, охорони та відповідальності, пов'язані з державною таємницею, регулюються Законом України «Про державну таємницю» від 21 січня 1994 р. На підставі ст. 12 цього Закону, Постанови Кабінету Міністрів України від 29 квітня 1994 р. № 278 «Про затвердження Положення про порядок і механізм формування та опублікування Зводу відомостей, що становлять державну таємницю» та відповідно до рішень державних експертів з питань таємниць, 1 березня 2001 р. наказом Голови Служби безпеки України № 52 був затверджений «Звід відомостей, що становлять державну таємницю».

«Комерційною таємницею є лише така інформація, яка відповідає певним вимогам, які, власне, і надають їй характер комерційної таємниці. Такими вимогами є: 1) комерційна цінність інформації; 2) секретність інформації; 3) вжиття заходів, спрямованих на збереження секретності такої інформації. Зазначені вимоги є тими критеріями, за допомогою яких, в разі порушення права на комерційну таємницю чи його оспорення, вирішується питання, чи існувало право на комерційну таємницю взагалі» [66, с. 88].

Слід визначити коло відомостей, яким необхідно надати статус комерційної таємниці. Саме ці відомості і будуть складати затверджений наказом керівника банку перелік відомостей, що становлять комерційну таємницю.

Після визначення і затвердження наказом керівника підприємства переліку відомостей, що становлять комерційну таємницю, визначаються конкретні заходи, які підприємство буде вживати для їх охорони. Серед них є розробка і затвердження: 1) правил внутрішнього трудового розпорядку; 2) положення про охорону комерційної таємниці; 3) інструкції про документообіг та роботу з документами; 4) посадових інструкцій про дотримання співробітниками режиму нерозголошення комерційної таємниці; 5) включення до тексту статуту підприємства розділів, які регламентують порядок охорони комерційної таємниці; 6) типової угоди про нерозголошення комерційної таємниці, яка укладається з особами, котрі мають доступ до такої інформації; 7) додаткової угоди до трудового договору чи контракту про нерозголошення найманими працівниками комерційної таємниці.

Раніше ми розглянули ризики банківських послуг. Ризикованими є більшість операцій банку, в т.ч. існує інформаційний ризик. Фахівці виділяють чотири види інформаційного ризику банку:

– ризик витоку і руйнування потрібної для функціонування банку інформації, особливо такої, що містить відомості таємного або конфіденційного характеру;

– ризик використання в діяльності банку необ'єктивної інформації;

– ризик відсутності у керівництва банку об'єктивної інформації;

– ризик розповсюдження будь-ким у зовнішньому середовищі невідповідної або небезпечної для банку інформації» [92, с. 31].

Досвід роботи українських банків із захисту таємниць від протиправних посягань показує, що залежно від суб'єкта посягання вони можуть бути зовнішніми та внутрішніми. Зовнішні посягання здійснюються конкуруючими банками, кримінальними елементами та іншими зацікавленими в цьому особами, внутрішні – працівниками банку, його акціонерами та клієнтами.

Співвідношення кількості інформаційних запитів з державних органів можна простежити на прикладі одного з українських банків за 1996-1998 рр. (додаток Б.6)

Найбільша кількість запитів до комерційних банків надходить від органів МВС, ДПА, СБУ та прокуратури (1996 р. – 69; 1997 р. – 63; 1998 – 80%), оскільки значна кількість злочинів економічного характеру знаходиться у провадженні саме цих органів [92, с. 35-36].

Запити державних органів стосуються різних категорій таємниць банку, в першу чергу, з категорії «відомості про клієнтів та партнерів» та «відомості про фінансову діяльність».

«Посягання конкурентів і кримінальних елементів на таємниці банків зумовлюються, як правило, їх боротьбою за розподіл зон впливу, встановлення домінуючого положення у відповідній сфері чи регіоні. Це пояснює періодичну циклічність випадків посягань з боку конкурентів і кримінальних елементів. Якщо запити державних органів надходять до банків відносно стабільно, то активність конкурентів і кримінальних елементів активізується щонайменше 2 рази на рік (навесні та восени).

Особливістю протиправних посягань на таємниці банків з боку конкурентів і кримінальних елементів є й те, що практично всі їх дії провадяться через або за сприяння працівників банків. Тобто внутрішні посягання, як правило, бувають не з ініціативи самих працівників банку» [92, с. 36].

Цікавими є дані спостережень щодо співвідношення загальної кількості намагань заволодіти таємницею банків і фактів, вдало доведених до кінця (додаток Б.7).

«Досвід показує, що аналіз посягання на таємниці банків ґрунтується на виявлених і, як правило, вдало проведених для злочинців і конкурентів фактах. Тобто кількість вдалих посягань на сьогодні значно перевищує кількість таких, яким запобігли або які перекрили системи захисту банків.

Що ж до протидії посяганням на таємниці банків, то тут юридична практика незначна. Застосування норм права для притягнення до

відповідальності осіб, винних у витоку інформації з обмеженим доступом, провадиться досить рідко. Це пояснюється тим, що, з одного боку, оприлюднення факту витоку інформації з обмеженим доступом може негативно позначатися на діяльності банку, і тому банки не прагнуть звертатись до правоохоронних і судових органів, а з іншого, як правило, слабкою буває доказова база. Тому хоча спроби подібного звинувачення були, однак все закінчується тим, що працівнику дають змогу звільнитися за власним бажанням або звільняють його за скороченням штату. Щодо зовнішніх посягань, то тут, як правило, банки обмежуються взаємним обговоренням фактів посягань та обіцянками дотримання чинного законодавства» [92, с. 36–37].

За посягання на комерційну та банківську таємниці може настати кримінальна, цивільна, адміністративна або дисциплінарна відповідальність, згідно із чинним законодавством. А це означає, що заходи захисту інформації повинні бути направлені на мінімізацію саме зазначених видів ризику.

Надання відповідним відомостям статусу банківської або комерційної таємниці є одним із способів запобігання несанкціонованому використанню цінної інформації.

Для комерційної таємниці важливим є охорона суті й змісту інформації, для банківської – не тільки суті відносин між банком і клієнтом, а й, як правило, самого факту наявності таких відносин. Комерційна таємниця може бути надана власником третій особі за плату. Надання банківської таємниці третій стороні є порушенням закону. Охорона комерційної таємниці – турбота її власника, а банківської – банку. Охорона банківської таємниці визначається не міркуванням прибутковості, а нормою закону. Для клієнта не має значення, з чиєї вини і за яких обставин стався витік інформації про стан його рахунку та банківські операції, у всіх випадках він направляє претензії до банку.

З прийняттям нового кримінального законодавства, який набув чинності з 1 вересня 2001 р. введено дві нові статті: ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю», і ст. 232 «Розголошення комерційної таємниці».

Статтею передбачена відповідальність за два склади злочинів: 1) незаконне збирання з метою використання відомостей, що становлять комерційну таємницю; 2) незаконне використання відомостей, що становлять комерційну таємницю, якщо це завдало великої матеріальної шкоди суб'єкту підприємницької діяльності.

Під незаконним збиранням відомостей, що становлять комерційну таємницю, слід розуміти активні дії, направлені на добування (одержання) таких відомостей будь-яким способом: вилучення, в тому числі викрадення

документів, що містять комерційну таємницю, чи предметів, відомості про які становлять комерційну таємницю; незаконне ознайомлення з такими документами чи предметами будь-яким способом; прослуховування телефонних розмов; опитування співробітників суб'єкта підприємницької діяльності; підслуховування усних розмов; одержання таких відомостей від осіб, які ними володіють, за плату чи шляхом застосування погроз, насильства тощо.

Під незаконним використанням відомостей, що становлять комерційну таємницю, слід розуміти впровадження «технічних» таємниць у власне виробництво, врахування здобутих відомостей при плануванні власної підприємницької діяльності, продаж відомостей, що становлять комерційну таємницю, їх розголошення тощо.

Оскільки кримінальну відповідальність ми розглянули в § 2.3. ІІ розділу, то тут згадаємо лише про цивільну, адміністративну та дисциплінарну відповідальність.

Цивільна відповідальність ґрунтується на цивільно-правових відносинах, за яких одна сторона зобов'язана відшкодовувати іншій збитки, завдані протиправними (і не завжди кримінально караними) діями у зв'язку з посяганням на комерційну (банківську) таємницю. Згідно зі ст. 203 ЦК УРСР збитки – це всі витрати, зроблені кредитором, втрата або пошкодження його майна, не одержані кредитором доходи, які б він одержав у разі виконання боржником своїх зобов'язань.

Адміністративна відповідальність за посягання на таємниці банку ґрунтується на положеннях Кодексу України про адміністративні правопорушення. Посягання на таємниці банку законодавство України відносить до дій, які кваліфікуються як недобросовісна конкуренція, що буде розглянуто в § 3.6.

Дисциплінарна відповідальність за посягання на таємниці банку ґрунтується на засадах трудового законодавства України та нормативної бази самих банків. В останньому випадку відповідальність можуть нести тільки працівники банку.

Отже, в теперішніх умовах відповідальність за незаконне розголошення або використання інформації, що становить банківську таємницю, передбачена тільки Кодексом про адміністративні правопорушення, а саме – ст.164[11] («Незаконне розголошення або використання інформації, що становить банківську таємницю»).

У Кримінальному кодексі передбачено відповідальність за незаконне збирання з метою використання відомостей, що становлять комерційну таємницю (ст. 231), за розголошення комерційної таємниці (ст. 232). Кримінальна відповідальність за незаконне розголошення або використання інформації, що становить саме банківську таємницю, відсутня.

Комітет Верховної Ради з питань законодавчого забезпечення правоохоронної діяльності свого часу рекомендував парламенту підтримати зміни до Кримінального кодексу України (щодо кримінальної відповідальності за незаконне збирання з метою використання відомостей, що становлять банківську таємницю, та за розголошення банківської таємниці).

Кодекс про адміністративні правопорушення передбачає відповідальність за незаконне використання інформації з обмеженим доступом щодо комерційної, банківської та державної таємниць, а Кримінальний кодекс – тільки щодо комерційної та державної таємниць, що не забезпечує належного захисту банківської таємниці.

Назріла потреба у посилення відповідальності осіб, яким банківська таємниця відома у зв'язку з професійною чи службовою діяльністю, за незаконне збирання з метою використання відомостей, що становлять банківську таємницю, та за розголошення банківської таємниці.

Як запевнив Голова Нацбанку ЗМІ на початку 2003 р.: «Після прийняття антивідмивочного закону Національний банк відпрацював програму, в якій розписано, що робить кожен департамент НБУ і банки щодо надання інформації стосовно операцій з клієнтами. Нацбанк навчить банківський персонал, і почнеться реальна робота: при цьому НБУ, беручи участь в цій програмі, не буде мати інформації, він буде лише збирати закодовану інформацію і передавати її у відповідний орган при Мінфіні. Останній після розкодування буде передавати комерційним банкам дані про те, що інформація одержана, і вони виконали норми закону. Після 10 червня ця схема вже повинна працювати як годинник. Після завершення цього терміну Нацбанк розпочне тотальні перевірки всіх до одного комерційних банків і філій на предмет дотримання законодавства про надання інформації уповноваженому органу».

Безперечно, готовність НБУ активно включитися в цю роботу не може не викликати загального схвалення. Але у авторів виникають з цього приводу деякі сумніви.

По-перше, НБУ «не буде мати інформації, він буде лише збирати закодовану інформацію і передавати...» Думається, що попередню професійну оцінку та узагальнення такої інформації слід роботи вже саме на цій стадії, а не зводити роботу такого важливого органу, яким є НБУ, до збирання і передачі інформації.

По-друге, є більш, ніж достатньо підстав для сумнівів, що (навіть з великою натяжкою) новостворений фінансовий підрозділ можна вважати розвідкою, навіть при всіх наданих йому юридичних і оперативно-розшукових повноваженнях. І взагалі, в Україні останнім часом дуже легко ставляться до терміна «розвідка», її статусу, створюючи масу відомчих

аналогічних підрозділів, окрім СБУ, – у ДПА, Миткомітеті, Міністерстві оборони, Службі охорони державного кордону, Управлінні державної охорони України тощо, а тепер – і в Міністерстві фінансів. Історичний досвід свідчить, що ефективніше ці проблеми вирішувала б одна розвідслужба (чи інший підрозділ), можливо при СБУ, оскільки замало оголосити тільки про створення розвідслужби. Головним завданням є забезпечеггя її професійними кадрами, матеріально-технічними, довідково-аналітичними можливостями, науковими установами, навчальними закладами. І де б такі підрозділи не створювалися заново, там не буде такого досвіду оперативно-розшукової роботи і відповідних можливостей в галузі розвідки, чи контррозвідки, який накопичено в СБУ. І що істотно, кожного разу при створені такої служби «викидаються» чималі суми коштів. А сконцентрувавши їх в одному місці можна досягти бажаного результату.

Загальновідомо, що надійність захисту комерційної і банківської таємниці залежить від продуманої системи безпеки.

Систему захисту банківської таємниці в Україні складають:

– загальні норми права із захисту секретної інформації, які встановлює держава (закони, декрети, укази, постанови);

– правові норми із захисту секретів, які встановлює керівництво банків (накази, розпорядження, інструкції, пам'ятки тощо);

– спеціальні структурні підрозділи банків, які на практиці забезпечують виконання норм, прийнятих державою та адміністрацією.

Всі ці елементи тісно пов'язані між собою. Так, банк може виробити самі досконалі правила та інструкції, які стосуються внутрішнього порядку поведінки з банківською таємницею, але за відсутності державно-правового регулювання не зможе захистити своїх секретів. Так само банк не зможе зберегти свої секрети, навіть за наявності правового регулювання, якщо не буде професійних фахівців цієї справи. Безпека, захист та охорона – єдина система. Банк не зможе зберегти своєї таємниці без реалізації механізмів та основних напрямів захисту секретів.

У банку мусить бути поставлена належна система контролю. Співробітники мають відчувати, що власники і працівники не послаблюють пильності щодо дотримання правил секретності та економічної безпеки в цілому. За порушення правил мусить бути суворе покарання. Кожна особа повинна усвідомлювати, що у випадку порушення інструкції у неї будуть серйозні неприємності.

Окремий режим встановлюються в організації роботи із захисту конфіденційної інформації щодо порядку поведінки з її носіями (документи, креслення, дискети, плівки тощо).

Суть його полягає в тому, що за відсутності працівника, на його робочому місці не повинно бути ніяких документів.

На західних фірмах з метою утруднення, або навіть неможливості копіювання закритих матеріалів вживаються додаткові заходи. Так, канадська фірма «Polimaik Management» розробила покриття для паперів, яке виключає можливість несанкціонованого копіювання нанесеного на них тексту.

Ще однією умовою збереження інформації є надійне її зберігання у неробочий час (сейфи, спецприміщення тощо). Кожен виконавець має зберігати у своєму сейфі тільки матеріали, за які він несе персональну відповідальність.

Значна втрата комерційної інформації відбувається під час ведення переговорів. Тому слід до переговорів чітко визначити, яку інформацію «засвітити» партнеру і яку залишити без висвітлення.

Сьогодні в промисловому шпигунстві широко використовують різного роду закладки (мікрофони, мініпередавачі тощо). У зв'язку із цим перед початком переговорів слід уважно перевірити приміщення, у яких вони будуть проводитися. Сьогодні є чимало спеціальних приладів, що здатні виявити такі закладки, встановити захисний екран, який виключає будь-яке прослуховування в таких приміщеннях.

На переговорах повинні бути присутніми тільки ті, кому це потрібно. Англійські спеціалісти з питань захисту інформації кажуть: «немає сенсу перевіряти перед переговорами те приміщення, де вони будуть відбуватися, якщо кава у це приміщення подається неперевіреним співробітником».

Багато таких питань доводиться розв'язувати банкам самостійно, оскільки законодавці не поспішають з прийняттям окремого закону, який би чітко регламентував усі аспекти комерційної таємниці.

Наразі, досить аморфне визначення цього поняття у ст.30 Закону «Про підприємства в Україні». Відповідно до ч.1 цієї статті, під комерційною таємницею підприємства маються на увазі відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, котрі не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам.

Далі законодавець установив, що перелік відомостей, які не можуть становити комерційної таємниці, визначається Кабінетом міністрів.

На виконання цього положення Кабінет міністрів 9 серпня 1993 р. прийняв постанову № 611, якою, власне, і визначив вичерпний перелік відомостей, що не є комерційною таємницею.

Таким чином, на сьогодні комерційну таємницю не становлять:

– установчі документи підприємств чи їх об'єднань;

– документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами (спеціальні дозволи, ліцензії, патенти, сертифікати, квоти тощо);

– інформація за всіма встановленими формами державної звітності (бухгалтерська, статистична);

– дані, потрібні для перевірки правильності обчислення і сплати податків та інших обов'язкових платежів;

– відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями, а також про наявність вільних робочих місць;

– документи про сплату податків і обов'язкових платежів;

– інформація про забруднення довкілля; недотримання безпечних умов праці; реалізацію продукції, що завдає шкоди здоров'ю; а також про інші порушення законодавства України та розміри заподіяних при цьому збитків;

– документи про платоспроможність;

– відомості про участь посадових осіб підприємства в кооперативах, МП, спілках, товариствах, об'єднаннях та інших організаціях, котрі займаються підприємницькою діяльністю;

– відомості, що відповідно до чинного законодавства підлягають оголошенню (наприклад, річні баланси комерційних банків).

Підприємство зобов'язане, на вимогу органів державної виконавчої влади, правоохоронних та контролюючих органів, а також інших юридичних осіб (відповідно до чинного законодавства), надавати зазначені вище відомості.

Водночас фахівці уточнюють: «Виходячи з того, що перелічена інформація не може бути комерційною таємницею, а деякі з відомостей потребують обмеженого доступу, слід пояснити таке: до форм державної звітності належать лише форми, встановлені Державним комітетом статистики України. Під документами про платоспроможність і даними, необхідними для перевірки обчислення податків, не можна розуміти документи і відомості, що стосуються операцій, рахунків і вкладів клієнтів та кореспондентів банку, оскільки вони згідно із Законом України «Про банки і банківську діяльність» (ст.52) віднесені до банківської таємниці. Як відомо, у разі неузгодження правових норм повинен спрацювати принцип верховенства закону над підзаконним актом. Відомості про чисельність і склад працюючих, їх заробітну плату не слід плутати з поіменним складом персоналу банку і матеріальним забезпеченням конкретних працівників.

Відомості про захист інформації, яка визначена постановою Кабінету Міністрів України № 611 як така, що не може бути комерційною таємницею, можуть отримати статус конфіденційної інформації, яка за Законом України «Про інформацію» (ст.30) також є інформацією з обмеженим доступом. Заходи захисту інформації в цьому випадку будуть обиратися керівництвом банку і ним же встановлюватиметься відповідальність за посягання на таку інформацію» [92, с. 17–18].

Цікавим є питання щодо права «інших юридичних осіб» вимагати від підприємства інформацію, котра, хоча і не є комерційною таємницею, може заподіяти йому збитки. Організація (підприємство, установа) має при цьому послатися на ту норму законодавства, яка прямо дозволяє їй таку інформацію витребовувати. Наприклад, таке право мають газети та журнали, відповідно до Закону «Про друковані засоби масової інформації» [139, с. 41].

Для того, аби підпадати під поняття «комерційна таємниця», інформація повинна:

– становити дійсну (фактичну) або потенційну цінність для підприємства з комерційних причин, витікання якої може зашкодити цьому підприємству;

– не бути загальновідомою або загальнодоступною на законних підставах;

– мати необхідний гриф;

– бути належним чином захищена;

– не бути державною таємницею;

– не бути захищеною авторським і патентним правом;

– не стосуватись негативної діяльності підприємства, котра може заподіяти шкоду суспільству і довкіллю.

Цілком закономірним є питання: чому об'єкти авторського і патентного права не становлять комерційної таємниці? По-перше, тому, що вони захищаються окремими законодавчими актами, і порушення авторського права досить легко довести. По-друге, будь-яка особа, сплативши певну суму за послуги Держпатенту, може офіційно отримати із «Державного реєстру свідоцтв України на знаки для товарів і послуг» витяг (інформацію) про будь-яке свідоцтво щодо знаку на товар чи послугу.

Відповідно до вже зазначеного Закону «Про підприємства в Україні», перелік і обсяг відомостей, які становлять комерційну таємницю, визначає керівник підприємства.

Загально визнано, що комерційною таємницею слід вважати відомості про:

– функціонування виробництва;

– плани перепрофілювання виробництва;

– організацію управління;

– перспективні плани розвитку;

– потребу в кредитах чи сировині;

– ділових партнерів, у т.ч. кредиторів;

– хід ділових переговорів;

– укладені контракти (договори, угоди);

– цінову політику;

– науково-технічні досягнення (якщо вони не захищені авторським чи патентним правом);

– організацію служби безпеки фірми.

У кожному конкретному випадку керівник підприємства може включати до цього переліку й інші, специфічні відомості.

Для того, аби зменшити ризик розголошення комерційної таємниці, на підприємстві має діяти чітка система безпеки.

Вона повинна включати:

– колективний договір і трудові контракти;

– інструкцію про порядок роботи з відомостями, що становлять комерційну таємницю;

– наказ про допуск працівників до відомостей, що становлять комерційну таємницю;

– пам'ятку працівника, який працює з такими відомостями.

Кожен працівник підприємства, котрий працює з інформацією, що становить комерційну таємницю, зобов'язаний:

– знайомитись тільки з тими відомостями і документами, до яких він дістав доступ на підставі своїх службових обов'язків;

– знати, кому із співробітників дозволено працювати з відомостями, що становлять комерційну таємницю, і в якому обсязі ці відомості можуть бути доведені до цих працівників;

– за участі в роботі сторонніх організацій, працівник може знайомити їх представника з відомостями, що становлять комерційну таємницю, лише з письмового дозволу керівника структурного підрозділу, у якому визначаються конкретні питання, котрі підлягають розгляду і вказується, кому і в якому обсязі може бути доведена інформація, що підлягає захисту;

– не розголошувати відомості, що становлять комерційну таємницю підприємства, які йому будуть довірені або стануть відомі по роботі;

– не передавати третім особам і не розкривати публічно такі відомості без згоди керівника підприємства;

– виконувати вимоги наказів, інструкцій і положень із забезпечення збереження комерційної таємниці підприємства, що стосуються працівника;

– при спробі сторонніх осіб одержати від працівника відомості про комерційну таємницю – негайно повідомити про це службову особу свого підприємства;

– зберігати комерційну таємницю тих підприємств, з якими встановлено ділові стосунки;

– при звільненні працівника всі носії комерційної таємниці підприємства (рукописи, чернетки, документи, креслення, друкарські стрічки, перфокарти, перфострічки, диски, роздрук на принтері (ксероксі), кіно-фото-негативи і позитиви, моделі, матеріали та інші відомості, що

визначені як комерційна таємниця), які були в його розпорядженні в зв'язку з виконанням службових обов'язків під час роботи у банку, передати уповноваженій особі або до відповідного підрозділу підприємства;

– про втрату або нестачу носіїв комерційної таємниці (посвідчень, перепусток, ключів від режимних приміщень, сховищ, сейфів (металевих шаф), особистих печаток та про інші факти, які можуть призвести до розголошення комерційної таємниці підприємства, а також про причини і умови можливого витікання відомостей, що становлять комерційну таємницю, негайно повідомити відповідну службову особу чи підрозділ підприємства.

На початку організації системи захисту необхідно виявити канали можливого витоку інформації. Практика показує, що найпоширенішими з них є:

– вивіз відходів і макулатури;

– спільна з іншими банками та фірмами економічна діяльність;

– фіктивні запити про можливість працювати на керівних посадах;

– відвідування фірм, показові семінари, екскурсії;

– інформація торгових представників фірм і торгових агентів про характеристику виробів;

– інформація, що розголошується консультантами й експертами;

– професійні заходи: симпозіуми, конференції, наради, семінари тощо;

– інформація, що направляється в ЗМІ;

– дії співробітників, ображених на керівництво банку;

– розмови й наради з конфіденційних питань у необладнаних приміщеннях;

– порушення режимних вимог.

З метою запобігання витоку банківської таємниці проводиться відповідна профілактична робота.

Під профілактичною роботою розуміється:

– виявлення найменших збоїв у роботі банку, розгляд їх як загрози економічній стабільності, аналіз тенденцій, причин, що викликали ці збої, уживання заходів щодо стабілізації роботи банку;

– виявлення найменших збоїв у роботі чи змін у стилі поведінки кожного співробітника, розгляд їх як можливої потенційної загрози цілісності системи захисту інформації, у разі потреби – вживання заходів з відновлення цілісності системи;

– добір співробітників на етапі кадрового набору, виходячи з принципів (критеріїв) безпеки;

– навчання персоналу основам загальної безпеки і захисту інформації;

– контроль виконання режимних вимог персоналом банку;

– виявлення серед персоналу банку потенційно небезпечних осіб, що можуть своїми діями зашкодити фірмі, й нейтралізація будь-яких передумов чи нелояльних дій співробітників.

До потенційно небезпечних відносяться особи:

– до яких можуть бути успішно використані вербувальні підходи;

– що працюють в інтересах інших фізичних чи юридичних осіб;

– незадоволені умовами роботи у банку (за матеріальними чи психологічними мотивами);

– пов'язані зі злочинними угрупованнями;

– не здатні виконувати вимог режиму внутрішньої безпеки фірми;

– не здатні до встановлення нормальних робочих комунікативних відносин зі співробітниками;

– психологія яких охоче допускає можливість помсти чи зрадництва.

Захист банківської інформації може опиратись і на норми трудового законодавства України, зокрема, на ті його положення, що передбачають встановлення трудових відносин на основі контрактів. Строк дії контракту та умови його розірвання встановлюються за згодою сторін, тобто відповідні заходи захисту банківської інформації можуть передбачатись у контрактах як одна із умов трудового договору. Нормативними актами, що регулюють встановлення трудових відносин працівника й адміністрації підприємства на контрактній основі, є постанова Кабінету Міністрів України від 19 березня 1994 р. № 170 «Про впорядкування застосування контрактної форми трудового договору» та наказ Міністерства праці України від 15 квітня 1994 р. № 23, яким затверджено Типову форму контракту. Основними положеннями цих документів є те, що контрактами можуть визначатись додаткові, крім встановлених законом, засади для його розірвання. Однією із таких додаткових засад розірвання трудового договору може бути завдання працівником матеріальної або моральної шкоди банку, в тому числі і шляхом протиправних посягань на інформацію з обмеженим доступом. Для практичного застосування таких умов слід виконати відповідні умови: укладення трудового договору у контрактній формі; включення до контракту умов, що передбачають його розірвання з ініціативи адміністрації банку у випадках, пов'язаних з протиправними посяганнями на банківську або комерційну таємницю чи конфіденційну інформацію банку; вина працівника банку у вчиненні таких дій [92, с. 31].

Це внутрішні умови збереження таємниці. Однак не менш важливими є зовнішні чинники.

Можна виділити дві основні категорії «мисливців» за комерційними секретами.

Перші – це конкуренти, для яких інформація про фірму дасть унікальні можливості витіснити банк з ринку.

Другі – спеціалізовані (часто нелегальні) агентства, бюро та інші заклади, для котрих одержання відомостей, що становлять комерційну таємницю, і торгівля цими відомостями є основним і єдиним джерелом існування.

Існує і третя група – представники організованої злочинності. Для них оволодіння комерційною таємницею означає повне і незаперечне підпорядкування банку або фірми своїм інтересам.

Наприклад, у США та Японії, за деякими джерелами, через витік інформації, фірми втрачають до 30% доходу.

Як правило, поставивши за мету розорити банк (чи поглинути його), фірма-конкурент чи інша зацікавлена організація розпочинає збір інформації. У цьому розділі не йтиметься про методи промислового шпигунства, а лише про те, які відомості попередньо (і легально!) збиратимуть про підприємство. Ці відомості становитимуть основу досьє на банк, фірму.

За дослідженням професора С.К. Реверчука, досьє на фірму складаються із таких основних блоків: карти фірми (базовий документ); відомості про переговори, якщо такі велися; інформація про результати, якщо такі виникли.

Карта фірми – базовий документ, котрий характеризує основні аспекти діяльності підприємства. До нього включають інформацію про:

– профіль фірми, рік заснування;

– власників та керівників;

– поштову, телеграфну адресу, телефони та електронні засоби зв'язку;

– філії, дочірні підприємства, участь в інших підприємницьких структурах;

– предмет торгівлі (виробництва) з фіксацією технічних характеристик;

– обсяги продаж (виробництва);

– кількість працівників, їх фаховий рівень, «ступінь відданості фірмі», матеріальне становище, звички, недоліки, відомості про сім'ю;

– найважливіших партнерів;

– стосунки з владними, контролюючими та правоохоронними органами, пресою;

– найважливіших конкурентів;

– негативні аспекти у діяльності фірми (невиконання зобов'язань, рекламації, арбітражні та судові справи, скандали тощо).

Особливу увагу фірма-поглинач надає розділу про власників, керівників та провідних фахівців підприємства. Перш за все, збиратиметься «відкрита» інформація: прізвища, домашні адреси, частка у статутному фонді (або кількість акцій), реальний вплив на управління фірмою. Потім – уподобання, звички, нахили, хобі тощо. Крім цього, добуватиметься інформація про особисте життя керівників та провідних фахівців.

Виявивши потрібну негативну інформацію про працівника, який має доступ до комерційної таємниці, зацікавлена організація зможе досить легко такою таємницею заволодіти.

Ще одним способом отримання відомостей, що містять комерційну таємницю, є публікації керівників чи спеціалістів у пресі, проведення так званих презентацій. Недарма і у нас, і на Заході напівжартома стверджують, що Японію побудували (в економічному розумінні) за допомогою ножиць.

Мається на увазі, що японські аналітики ретельно вивчали і копіювали публікації з журналів типу «Наука и жизнь», «Юный техник». Тому, публікуючи матеріал про фірму, належно відредагуйте його.

Проте суто запобіжних, попереджувальних заходів недостатньо для збереження комерційної таємниці. Потрібне активне втручання держави. У різних країнах ця проблема вирішується по-своєму.

Наприклад, у Великій Британії це питання регулюється в рамках більш загальної категорії конфіденційності, нормами договірного права, деліктного права, судовими прецедентами та окремими нормативними актами.

У Німеччині обов'язок не розголошувати таємницю особою, котрій вона стала відома через її службове становище чи роботу, передбачається в багатьох законодавчих актах. Такий обов'язок установлюється законом для працівників як державних установ федерації й земель, так і для службових осіб та службовців, робітників фірм і корпорацій.

У Франції захист інтересів підприємців у сфері комерційних секретів забезпечується застосуванням загальних положень кримінального, трудового та цивільного законодавства, які регулюють відповідно питання збереження професійних секретів, звільнення, відшкодування збитків.

У Швейцарії законодавчі норми з порушених питань містяться в різних нормативних актах: кримінальному кодексі, трудовому праві, патентному законі, законі про оподаткування, законі про несумлінну конкуренцію та ін. Причому в законодавстві містяться лише головні принципи. Інші питання, включаючи предмети і процеси, що становлять об'єкт таємниці, вирішуються керівництвом банків, підприємств і фірм.

За законодавством Фінляндії у разі розголошення чи передачі конкуренту або третім особам комерційних відомостей можуть застосовуватися відповідні параграфи Закону про неправомірні угоди, а також Кримінального кодексу.

Зазначене дозволяє зробити висновок, що з правового погляду комерційна таємниця у світовій практиці становить засіб захисту проти несумлінної конкуренції в рамках реалізації права на інтелектуальну власність.

Аналізуючи законодавство зазначених країн про відповідальність за розголошення комерційної таємниці, професор С.К. Реверчук виділяє такі спільні для них моменти.

«По-перше, у більшості з них за розглядувані правопорушення передбачається позбавлення волі від кількох місяців до двох років. Суворі

наслідки настають при передачі комерційної таємниці за кордон – це діяння однозначно кваліфікується як промислове шпигунство.

По-друге, розмір штрафу часто не визначений у нормах закону і встановлення його віднесено до компетенції суду.

По-третє, за позовом потерпілого чи відповідного державного органу суд може зобов'язати винного до відшкодування заподіяної шкоди не лише у вигляді збитків, але й включити до неї упущену вигоду та моральну шкоду.

По-четверте, зарубіжне законодавство містить перелік й інших можливих санкцій за порушення умов конфіденційності комерційної таємниці, до якого входить: вилучення чи знищення документа або предмета, котрий містить таємницю; знищення матеріальних засобів, якими здійснювалася протиправна діяльність; припинення порушення; заборона незаконної діяльності; закриття підприємства; публікація судового рішення» [139, с. 49].

Обов'язковою ознакою об'єктивної сторони незаконного використання відомостей, що містять комерційну таємницю, є наслідки у вигляді заподіяння великої матеріальної шкоди суб'єкту підприємницької діяльності, тобто шкоди, яка в п'ятдесят і більше разів перевищує встановлений законодавством мінімальний розмір заробітної плати. При визначенні розміру заподіяної шкоди слід врахувати прямі матеріальні збитки, витрати на відвернення шкідливих наслідків, використання відомостей іншими суб'єктами підприємницької діяльності, збитки від зниження реалізації продукції і товарів чи зменшення попиту на послуги, затрати на перепрофілювання напрямів діяльності, збитки від змнешення цін на товари і послуги тощо. Заподіяння моральної шкоди суб'єкту підприємницької діяльності внаслідок використання відомостей, що містять комерційну таємницю (наприклад, підрив ділової репутації), на кваліфікацію не впливає, але має враховуватися у разі призначення покарання.

Цією статтею передбачена відповідальність у вигляді позбавлення волі на строк до трьох років чи штрафу від 300 до 500 мінімальних заробітних плат.

Встановлено відповідальність за розголошення комерційної таємниці. При цьому законодавець зробив наголос ось на чому.

Законом України від 2 жовтня 1992 р. «Про інформацію» проголошено правовий захист інформації з обмеженим доступом, різновидом якої є конфіденційна інформація – відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. До конфіденційної інформації відносяться і відомості, що становлять комерційну таємницю суб'єкта підприємницької діяльності.

Розголошення комерційної таємниці – це незаконне ознайомлення інших осіб з відомостями конфіденційного характеру, віднесеними суб'єктом підприємницької діяльності до відомостей, що становлять його комерційну таємницю, а так само умисне створення умов, які сприяли ознайомленню з ними сторонніх осіб, вчинене особою, котрій такі відомості стали відомі у зв'язку з професійною чи службовою діяльністю і яка повинна зберігати такі відомості в таємниці.

Способи розголошення відомостей, що становлять комерційну таємницю, можуть бути різними: повідомлення вказаних відомостей іншим особам, зокрема, конкурентам; надання іншим особам для ознайомлення документів, що містять комерційну таємницю; повідомлення відомостей, що містять комерційну таємницю, в засобах масової інформації тощо.

Цією статтею передбачена відповідальність у вигляді позбавлення волі на строк до двох років або виправних робіт на строк до двох років, або позбавлення права займатися певною діяльністю чи займати певні посади (до 3-х років), або штраф до 50 мінімальних розмірів заробітної плати.

Чинний Цивільний кодекс містить наступне поняття комерційної таємниці: «Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці» [184, с. 159].

Але питання банківської таємниці залишається поки що не врегульованим.

Аналіз практики захисту [67, с. 47–49] банківської таємниці в зарубіжних країнах показує, що коли слід в банках різних країн світу отримати майно, що належить Україні, але знаходиться за межами України, цю проблему можна вирішувати з дотриманням таких вимог: наявності меж спеціальної охорони банківської інформації; існування державно-правових домовленостей про взаємодію в правовій сфері.

Слід враховувати, що практично в усіх країнах світу відомості про банківські рахунки і операції – банківська таємниця. А тому відомості про рахунки можна отримати, як правило, тільки у разі порушення кримінальної справи стосовно тієї чи іншої особи. Провадження цивільної справи в багатьох країнах (Німеччина, Франція та інші) не дає підстав для

передачі банком судовим органам будь-яких відомостей, за виключенням тих ситуацій, коли банк сам є зацікавленою стороною у справі.

В Англії суд має право вимагати від банку надання копій рахунків клієнта, а також зобов'язати банк надати цю інформацію іншим представникам держави, податковим інспекторам.

У США норми права зобов'язують банки належним чином вести облік документів щодо рахунків клієнтів і повідомляти про угоди, які перевищують суму в 10 тис. доларів.

У Швейцарії, князівстві Ліхтенштейн, Австрії та Люксембурзі охорона банківської інформації розглядається як одна з найважливіших задач, а тому отримати будь-які відомості з банку практично неможливо, а правовими актами передбачається видача банківської інформації лише у випадку вчинення злочину. Необґрунтована передача такої інформації тягне за собою суворе кримінальне покарання банківських службовців (до 20 років позбавлення волі) [67, с. 47–48].

Всі розглянуті раніше проблеми стосуються людей і залежать від них, що зумовлює потребу, насамкінець, розкрити практику банківського менеджменту і роботи з персоналом банків.

3.7. Практика банківського менеджменту та роботи з персоналом банків, їх роль у забезпеченні безпеки банків і банківської діяльності в Україні

У науковому обігу і практиці усе частіше стало використовуватися поняття «менеджмент», яке поступово витісняє загальновизнане поняття «управління». У кожній галузі це поняття має власне значення і відтінок.

Стосовно до банківської системи, зокрема, у «Російській банківській енциклопедії» термін «менеджмент» (управління, завідування, організація) визначається як управління підприємством (фірмою) в умовах ринкової економіки, спрямоване на вибір оптимального способу одержання найвищих економічних результатів [161, с. 107]. Не важко помітити, що це надто загальне визначення зазначеного поняття і не відтворює його змісту, особливо в банківській системі.

В основі кадрового менеджменту лежить кадрова політика банку. **Сучасна кадрова політика** є багатосуб'єктною і визначається, насамперед, як генеральна лінія, котра забезпечує виявлення наукових принципів підбору, розстановки і використання кадрів управління, визначення зумовлених конкретними історичними умовами, вимог до них, а також завдань, напрямів, форм і методів кадрової роботи.

Кадрова політика на практиці проводиться за допомогою певної системи, що містить окремі дії та операції, а саме: планування і прогнозування потреб у кадрах, їх підбір, оцінка, розстановка, виховання, підготовка, контроль тощо. Основу цієї системи складають підбір і розстановка кадрів, які забезпечують їх оновлення. Життям неодноразово перевірена сентенція: кадри без оновлення, все одно, що колодязь без джерела. Адже для того, щоб кадри вирішували все, вони повинні бути початково-спонукальною, тобто рушійною, силою всіх процесів розвитку і постійно розвиватись.

Основними засадами і загальними правилами роботи з кадрами є принципи їх підбору. Серед них в умовах державотворення чільне місце посідають такі, як професійна компетентність; дієздатність та ефективність; беззастережне служіння інтересам українського народу; наявність організаторських здібностей, доброчесність і відповідальність; вмотивованість і престижність банківської праці; послідовне оновлення кадрів на основі спадкоємності, співпраці досвідчених і молодих працівників; соціальна справедливість; оновлення, гласність і колегіальність у вирішенні кадрових питань; підготовка таких керівних кадрів, котрі б знали історію, культуру, державну мову, традиції України.

В організації роботи з керівними кадрами важливу роль відіграє правове регулювання як на загальнодержавному, так і банківському рівнях. Право, з огляду на імперативні правові норми, в цьому випадку є регулятором взаємовідносин між органом управління і працівниками. Останнім часом проведена значна законодавча і нормотворча робота щодо формування управлінської й кадрової системи, здатної автономно функціонувати в умовах суверенітету України. Проте тут не вдалося уникнути серйозних помилок і прорахунків, що сьогодні гальмує розвиток та реформування системи управління, в т.ч. БСУ. Чинна нормативно-правова база ще не має єдиного концептуального підходу до процесу формування і реалізації чіткої кадрової політики. Окремі законодавчі акти не спрацьовують, вони не підкріплені потрібною матеріально-технічною базою, кадровим забезпеченням. Чітко не визначені суб'єкт управління і його повноваження на всіх державних рівнях. Окремою проблемою є правове регулювання кадрової політики в умовах переходу до ринкової економіки і появи приватної власності, що охоплює переважно імперативне й методичне регулювання взаємовідносин між суб'єктом і об'єктом управлінської діяльності.

Аналіз теоретичних та практичних проблем управління і кадрового менеджменту дав змогу простежити їх генезис. Кадровий менеджмент одержав широке визнання у світі, адже він найбільше відповідає потребам та умовам ринкової економіки, є антиподом командно-адміністративного,

авторитарного управління. Основними його ознаками як типу управління персоналом вважаються: у центрі управління має бути людина з її потребами, інтересами, мотивами, цінностями; перевага надається економічним методам і засобам управління; професіоналізм управління – одна із головних вимог до менеджера; гнучка організація управління здатна швидко змінюватися відповідно до змін середовища. Таким чином, ця діяльність створює психолого-юридичні відносини між об'єктом і суб'єктом управління, сприяє досягненню поставлених цілей шляхом використання мотивів праці та інтелекту людей.

В нових умовах пріоритет має належати фахівцям-управлінцям, створенню ефективної структури і системи управління, оновленню його функцій та методів.

Отже, сучасні управлінці мають повною мірою володіти методологією управлінської діяльності, причому адекватною рівням управлінням із забезпечення економічної і банківської безпеки, за тими посадами, які вони обіймають. Якщо на нижчих рівнях достатньо володіти відповідними прийомами, формами і методами впливу на підлеглих, то на верхніх, – звідки провадиться керівництво всією системою, управлінці не можуть обійтись без грунтовної політичної і фінансової компетенції, адже вони повинні прогнозувати розвиток подій та кваліфіковано регулювати їх.

Система управління, де керівник відіграє організуючу роль персоніфікованого керівництва, висуває до нього певні вимоги. Суть цих вимог полягає в тому, що для успішного управління діяльністю підлеглих керівник повинен володіти відповідними знаннями і вміннями, певними морально-етичними, діловими та особистими якостями, бути беззастережно відданим інтересам своєї держави і справи. Обсяг цих вимог є синтезованим і включає як ті, що висуваються до керівних кадрів апарату державного управління, так і до державних службовців. Ці вимоги змінюються адекватно економічному розвитку держави і суспільства.

Застосуванню на практиці наукових засад визначення залежності вимог, що висуваються до керівника, від характеру його діяльності і службового становища сприяє концепція побудови професійно-кваліфікаційної моделі сучасного керівника. Розроблена нами модель складається з двох частин. Перша містить функції керівника у сфері адміністративно-управлінської і професійно-фінансової діяльності. Друга – кваліфікаційні вимоги до морально-етичних, ділових, особистих якостей, знань і вмінь керівника.

Вітчизняна практика свідчить, що всебічному вивченню особистості до призначення на посаду сприяють такі методи вивчення, як соціальне моделювання, психофізіологічне обстеження і психодіагностичне тестування, що сучасний стан науки дозволяє втілювати в життя з високою

ефективністю. Організаційно-правові та інструментарно-методичні можливості направляються на вирішення профорієнтаційних, профконсультаційних, профвідбірних та профадаптаційних завдань. Досвід переконує, що все це за умов гласності і колегіальності прийняття рішень щодо визначення відповідності особи посаді сприяє недопущенню в підборі і розстановці управлінської еліти фактів протекціонізму, користолюбства, незаконного лобізму, кадрового і банківського ризику.

Сьогодні всі автори пропозицій щодо шляхів виходу держави з кризи при широкому розмаїтті ідей одностайні в думці: відродити Україну зможуть лише професійно компетентні люди, патріоти з високим почуттям громадянського обов'язку.

Отже, стан економічної безпеки України, сучасне і майбутнє її державності прямо залежить від формування управлінської банківської еліти. Підбір і розстановка таких кадрів повинні здійснюватись у суворій відповідності до вимог, які до них висуваються, згідно із сучасною кадровою політикою, її засадами.

Можна погодитися з певним застереженням із визначенням, що «банківський менеджмент – це наукова система управління банківською справою і персоналом, зайнятим у банківській сфері, що визначає цільові настанови в діяльності банку і створює механізм їхньої реалізації, а також характеризує якість управління банком, тобто ефективність організації та керівництва банком в умовах, що постійно змінюються» [161, с. 108].

Тут, по-перше, ставиться знак рівності між банківським менеджментом і системою управління, навіть якщо вона наукова. По-друге, банківська система України (як і Росії) ще дуже молода і рано говорити про наукову систему управління банківською справою, тим більше опанування фундаментальними і науковими досягненнями, що стали загальним надбанням. Адже молода наука ще не знає відповіді на багато питань, рішення слід приймати вже сьогодні, практику потрібні чітко сформульовані рекомендації, що випливають з результатів наукового дослідження і узагальнення практики. Отже, чималу відстань від теорії менеджменту до прикладного управління ще належить подолати.

Тому **банківський менеджмент**, на наш погляд, слід трактувати і як управління банківською системою (банківською справою), і як управління персоналом (його кадрами). Банківський менеджмент – це практика управління банківською системою і банківською справою, а також персоналом банків на основі нормативно-правового регулювання цієї діяльності як на загальнодержавному, так і банківському рівнях сучасної кадрової політики відповідно до принципів, форм і методів управління.

Такий підхід до організації банківського менеджменту загалом дозволяє підпорядкувати управління БСУ банківському менеджменту, або управляти банківською системою через персонал.

У підсумку банківський менеджмент визначається як «управління всіма процесами і відносинами (фінансовими, економічними, трудовими, техніко-технологічними, організаційними, правовими, соціальними й ін.), що характеризують діяльність банку» [161, с. 109]. Не важко помітити, що з цього визначення «випав» кадровий менеджмент, який має немало особливостей саме у банківській системі та складає основу, становий хребет всієї системи управління БСУ.

З численних публікацій на цю тему відомо, що управління банком їх авторами в більшості випадків розглядається як управління фінансами банку [161, с. 109]. Але за такого підходу не охопленою залишається ціла система інших аспектів, зокрема й персонал.

Загальновідомо, що не можна управляти банком та його фінансами не управляючи працюючими людьми, і навпаки. Сприймаючи позицію М.В. Туленкова, що «Банк без персоналу і банківський персонал поза банком, що допускається у формулюваннях типу «управління фінансами банку і його персоналом» – суцільна нісенітниця» [161, с. 109], слід все ж зазначити, що це хоча і нерозривні, проте і не ідентичні поняття, які вимагають організації властивого лише їм процесу управління. Адже «ефективне функціонування банківської системи, її збалансований, пропорційний розвиток значною мірою залежить від наявності ще і такої важливої ланки, як інфраструктура, яка становить сукупність допоміжних елементів, що забезпечують нормальну діяльність кредитних установ, сприяючи функціонуванню складного механізму взаємозв'язків банків з суб'єктами економічних відносин, що діють у різних секторах господарства країни.

В Україні створення дворівневої банківської системи відбувалося в історично стислі строки, а тому потрібна інфраструктура ще не сформувалась як закінчена [102, с. 96]. На практиці організаційно вона має забезпечувати реалізацію допоміжних функцій через елементи, що у нормальних ринкових умовах мають охоплювати інформаційне, технічне, науково-методичне, кадрове та законодавчо-правове забезпечення діяльності банків.

Інформаційне забезпечення організує діяльність різноманітних спеціалізованих організацій, що визначають рейтинги банків, проводять аудит їхньої діяльності, провадять аналіз та надають інформацію про стан банківської системи у власних інформаційних виданнях, створюючи можливість для зацікавлених отримувати повну інформацію про функціонування банківської системи, надійність, прибутковість, ефективність управління в окремих банках.

Оскільки такі структури утворені державою, вони можуть існувати на пайових засадах з групою банків для забезпечення їхніх потреб у даних з питань економічного розвитку країни на макро- та мікрорівні.

Технічне забезпечення задовольняє банки усім потрібним обладнанням для обслуговування клієнтів, розробляє і впроваджує певне програмне забезпечення, налагоджує і обслуговує канали зв'язку для оперативної передачі інформації та реалізації фінансових угод, а також забезпечує надійний захист зазначених каналів від несанкціонованого доступу, формує міжбанківські розрахункові (клірингові) центри для оперативного врегулювання взаємних зобов'язань.

Науково-методичне забезпечення передбачає розробку для банків методики проведення окремих видів операцій, управління активами і пасивами, формування оптимальних портфелів вкладень, мінімізації ризиків тощо. Адже НБУ не в змозі виконувати повною мірою ці функції.

Кадрове забезпечення діяльності банківської системи покликане своєчасно і якісно провадити підбір, підготовку, розстановку, виховання, ротацію банківських службовців. У кількісному відношенні цю проблему практично вирішено, але тепер постає питання якості підготовки фахівців, що вимагає створення мережі різноманітних навчальних закладів, узгодження навчального процесу із сучасними запитами банків.

Законодавчо-правове забезпечення банківської діяльності передбачає створення належного правового поля, що є вихідним положенням у забезпеченні стабільного функціонування усіх банків. Сукупність чинних законодавчих актів має регулювати не лише загальні моменти діяльності кредитних установ, як тепер, а й окремі аспекти банківської справи в країні (кредитної, депозитної, інвестиційної) та основ діяльності різних елементів банківської системи (зокрема, спеціалізованих комерційних банків різних видів) тощо.

Без сукупності розглянутих елементів інфраструктури нормальне функціонування банків в умовах ринку неможливе або вкрай ускладнене. Тому створення відповідного забезпечення організації банківської справи за різними напрямами слід вважати одним із моментів подальшого вдосконалення інституційної структури банківської системи. Слід нормативно інтегрувати до банківської системи зазначену сукупність складових, які формують інфраструктуру, що об'єктивно випливає із необхідності всебічному регулюванні діяльності банківської системи.

Забезпечення безпеки українських банків регламентується чинним законодавством, внутрішніми нормативними актами. Останні видаються відповідно до форм реалізації заходів безпеки: охорони, режиму та інформаційно-аналітичного забезпечення діяльності банку.

Комерційні банки вживають заходів безпеки власними силами. У статутах передбачається, що банки мають право на комерційну таємницю, конфіденційну інформацію і їх захист, на охорону своєї власності.

Банки, як правило, розробляють Концепцію безпеки банку. Вона містить:

– загальні положення (основні поняття і терміни, характеристику умов діяльності банку та загроз йому, мету, завдання і принципи безпеки);

– заходи організації безпеки банку (планування та організація вживання заходів безпеки, функції підрозділів банку з питань безпеки, відносини між підрозділами, із суб'єктами підприємництва, державними органами при забезпеченні захисту інтересів банку, структура підрозділу безпеки банківської діяльності, її функції, права і відповідальність, роль і завдання охоронних і детективних фірм, послуги яких використовуються для забезпечення безпеки банку, порядок комплектування та підготовки співробітників підрозділу безпеки, забезпечення взаємодії з правоохоронними органами);

– заходи безпеки банку (перелік основних заходів, форми і методи їх виконання, дії банку за непередбачених умов і в екстремальних ситуаціях);

– забезпечення безпеки банківської діяльності (кадрове, фінансове, матеріально-технічне, науково-методичне, інформаційне та ін.).

На основі цієї Концепції банки розробляють Положення про підрозділ безпеки та інші документи щодо вживання заходів безпеки:

а) з питань охорони.

На основі наказу про призначення комісії з огляду об'єктів банку щодо організації їх охорони власними силами, результати роботи комісії оформляються актом, у якому зазначається стан об'єктів та даються рекомендації щодо організації їх охорони: вид охорони, кількість постів охорони, заходи щодо створення штучних бар'єрів доступу у банк тощо. На основі акта розробляються заходи охорони та створюється Дислокація – документ, де вказується порядок охорони об'єктів банку технічними засобами та фізичними силами. Завершальним і відповідно основним нормативним актом банку з питань його охорони є наказ про затвердження інструкцій про пропускний і внутрішньооб'єктовий режим та режим функціонування і охорони касового вузла. Цими документами передбачається порядок доступу персоналу, клієнтів, акціонерів та відвідувачів у банк, застережені дії протипожежної безпеки, порядок здачі під охорону приміщень, поведінка персоналу і сил охорони за непередбачених обставин та ін. Крім того, для дій в екстремальних умовах у банках розробляються так звані кризові плани, які погоджуються з місцевими органами міліції.

б) з питань режиму.

Згідно із законами України «Про підприємства в Україні» і «Про інформацію» в банку організується робота з визначення та підбору відомостей, які становлять комерційну таємницю та конфіденційну інформацію банку. З метою нормативного їх закріплення видається наказ,

яким затверджується Положення про інформацію банку з обмеженим доступом. Положення передбачає перелік відомостей, що становлять комерційну таємницю та конфіденційну інформацію банку, склад осіб, яким ці відомості можуть доводитись у повному обсязі, заходи захисту відомостей, що становлять комерційну, банківську таємницю та конфіденційну інформацію. Положенням також встановлюється відповідальність за розголошення інформації з обмеженим доступом.

Крім цього, до нормативних документів з режиму банку також належать: внутрішній розпорядок роботи банку; Положення про трудову дисципліну; Положення про службове діловодство; Положення про проведення службових розслідувань; положення, інструкції, що регламентують захист інформації в автоматизованих інформаційних системах та мережах банку, порядок доступу до неї; інструкції для посадових осіб про тримання у таємниці відомостей, які їм стали відомі при виконанні посадових обов'язків і які становлять інформацію з обмеженим доступом; зобов'язання працівників банку щодо нерозголошення відомостей, які становлять інформацію з обмеженим доступом; угоди про конфіденційність, укладені з клієнтами і партнерами банку; окремі положення Інструкції про порядок комплектування персоналу банку [92, с. 20–21].

Аналіз результатів діяльності банків з питань безпеки показує, що не всі банки створюють повну нормативну базу. Відсутність законодавчої і нормативної бази з цих питань часто не дає можливості банкам не тільки регламентувати таку діяльність власними нормативними актами, а й активно провадити її.

Як повідомив В. Артемьєв у «Довіднику кадровика» всередині фірми чи банку ведеться своя контррозвідувальна робота [136]. До завдань служби безпеки фірми входить швидке й адекватне реагування на будь-які дії, що здатні дестабілізувати її роботу. Усередині фірми цими питаннями займається спеціальний підрозділ (контррозвідка банку). Іноді таку структуру називають службою захисту інформації.

На підрозділи СБ банків покладаються такі завдання: організація режимів конфіденційного діловодства, допуску співробітників і сторонніх осіб до конфіденційної інформації, безпеки проведення ділових нарад і переговорів, зберігання, обліку і знищення носіїв конфіденційної інформації й ін.; виявлення каналів можливого витоку інформації, їхня нейтралізація; профілактична робота і проведення службових розслідувань; протидія технічним засобам промислового шпигунства (економічній розвідці інших підприємств і фірм, інших фізичних чи юридичних осіб); проведення спеціальних акцій, спрямованих на створення сприятливої обставини і нормалізації функціонування власного підприємства; зв'язок зі службами безпеки інших фірм і державних структур; взаємозв'язок із

засобами масової інформації (ЗМІ). При цьому слід враховувати, що відповідно до Закону України «Про інформацію» у банку існують такі її види: інформація з обмеженим доступом (відноситься до державних таємниць або конфіденційна); інформація, що є власністю держави; відкрита інформація.

Чільне місце в організації надійного захисту закритої інформації належить роботі з кадрами. Експерти вважають, що надійний захист секретів фірми на 80% залежить від правильного підбору, розстановки і виховання кадрів. Робота ця має розпочатися при прийомі людини на роботу, а обов'язок зберігати таємницю має стати умовою контракту.

Італійські психологи стверджують: із всіх службовців фірми тільки 25% по-справжньому чесні люди. Інші 25% тільки й чекають випадку, щоб розповісти про виробничі таємниці, а 50% будуть діяти залежно від обставин.

Іншим напрямом роботи з кадрами є обмеження доступу до секретної інформації. Тут повинен діяти принцип – кожен працівник має доступ лише до тієї інформації, яка потрібна йому для виконання своїх службових обов'язків.

Важливим напрямом роботи з кадрами є проведення виховної роботи. Американські фахівці з питань протидії комерційному шпигунству дають власникам фірм такі рекомендації:

– використовувати будь-яку можливість і ситуацію для пропаганди програм забезпечення секретності;

– періодично нагороджувати співробітників фірми за успіхи в захисті секретної інформації;

– стимулювати зацікавленість працівників фірми у виконанні програм секретності.

Значне місце у виховній роботі з кадрами посідає навчання працівників. Основними цілями навчання є:

1) чітке знання співробітниками видів і обсягів секретної інформації, за збереження якої вони несуть особисту відповідальність;

2) розуміння виконавцем секретних робіт характеру і цінності даних, з якими він працює; усвідомлення можливих способів і методів проникнення до даних, якими міг би скористатися порушник;

3) навчання встановленим правилам і процедурам захисту й зберігання закритої інформації [139, с. 37].

Як показує практика роботи в сфері безпеки, керівникам дуже корисно розробити систему гласних заохочень. Потрібно поєднувати систему заохочень з питаннями безпеки. Кожен член колективу має усвідомити (і перевірити на собі), що будь-яка дія, що зміцнює безпеку фірми, її економічну стабільність, буде гідно нагороджена.

Базовим видом діяльності у профілактичній роботі є виховна робота та турбота про людей. Саме фахівці з безпеки повинні навчити кожного співробітника банку основам безпеки комерційної діяльності. У першу чергу навчання мають пройти співробітники, що працюють з конфіденційними чи матеріальними цінностями.

Аналіз діяльності банків дозволяє стверджувати, що служба безпеки повинна відслідковувати будь-які зміни в економічній стабільності банку, у мікрокліматі колективу, у поведінці кожного із співробітників, тому що вони можуть мати серйозні наслідки.

Співробітники служби безпеки повинні бути не тільки органом, що «забороняє», бо роль «шлагбаума» малопродуктивна. Вони повинні разом зі співробітниками відділів активно шукати виходи, поліпшувати режим, вживати націлених на це заходів. Ідеї безпеки повинні стати загальними, а не бути нав'язливою рекомендацією служби.

Співробітники безпеки, аналізуючи діяльність когось з фахівців інших служб, що підозрюється в нелояльності до фірми, повинні діяти обережно, акуратно, не зачіпаючи гордості, почуття власної гідності підозрюваного, аж до моменту безперечного установлення факту нелояльності. Потреба у такій делікатності зумовлена такими причинами: підозрюваний може бути і не винен, а образа підштовхне його на крайні міри з заподіянням максимальної шкоди кривдникам; якщо факт нелояльності встановлений, стає можливою тонка контргра (наприклад, запуск дезінформації).

У боротьбі за клієнта важливу роль відіграє високий професіоналізм службовців і здатність банку забезпечити зберігання банківської таємниці. Клієнт надає перевагу саме тому банку, в якому запропонують професійне, швидке, приємне і вигідне обслуговування. А це залежить насамперед від того, як підібрано кадри у банку, рівня професійної підготовки, практичного досвіду. Практика свідчить [99, с. 55], що факторами ризику, здатними поставити під сумнів репутацію будь-якого банку, є: некомпетентність, неуважність його працівників, недостатній рівень їх освіти та загальної культури. У разі прийому на роботу непорядної людини, банк може понести великі фінансові збитки внаслідок умисних дій чи навіть бездіяльності такого працівника.

В процесі підбору персоналу найважливішу роль відіграє кадрова служба банку, яка по суті є першою інстанцією у боротьбі за високий рівень банківської установи.

Для банківського менеджменту важливо враховувати організаційну структуру банку. Вищим органом управління є Загальні збори учасників. З числа учасників банку обирається Спостережна рада. Виконавчим органом, який безпосередньо управляє його поточною діяльністю, є Правління (Рада директорів) банку. Контроль за фінансово-господарською діяльністю

виконує ревізійна комісія. Всі ці органи функціонують на підставі Статуту банку, Закону України «Про банки та банківську діяльність», відповідних положень.

Управлінням банківської установи, в тому числі й кадровими питаннями, займається Правління банку. На засіданнях Правління приймається та затверджується штатний розпис та вносяться зміни до нього. Очолює Правління голова, який діє від імені банку в межах, визначених його Статутом. Контроль за основними напрямами діяльності банку покладено на головного бухгалтера та заступників голови Правління.

До основних підрозділів банку належать такі управління (департаменти, сектори тощо): бухгалтерське, операційне, внутрішнього аудиту, юридичне, клієнтське (операційне, валютне), активно-пасивних операцій; безпеки. У свою чергу, вони поділяються на більш дрібні сектори, відділи. Кожний з підрозділів очолює керівник відповідного рівня. В деяких випадках дрібний підрозділ виводиться зі складу більш великого і підпорядковується безпосередньо Правлінню.

Всі банківські посади можна умовно поділити на три типи: керівники найвищого рівня (так звані топ-менеджери) – голова та члени Правління, головний бухгалтер тощо; керівники середньої ланки – начальники управлінь, секторів, відділів, служб тощо; рядові співробітники [99, с. 55].

До кожної категорії працівників висуваються певні вимоги, деякі з них затверджені законодавчо, інші встановлює сам банк з метою отримання найвищих професійних результатів праці та безпеки своєї установи.

Основними етапами у процесі підбору персоналу є: безпосередній пошук працівника, перевірка його відповідності вакантній посаді, прийом на роботу. На першому етапі роботу виконує кадрова служба банку, на другому – кадрова служба, служба безпеки, керівник відповідного підрозділу, на третьому – керівник, який приймає рішення про зарахування, кадрова та юридична служби, що оформляють працівника на роботу.

Насамперед слід сформувати вимоги до якостей та знань майбутнього працівника: стосовно віку, статі, сімейного стану, стажу роботи, які встановлює керівник, що приймає рішення про майбутнє зарахування працівника. Вимоги до освіти та стажу роботи містяться у внутрішніх банківських посадових інструкціях. Деякі специфічні вимоги до окремих категорій працівників встановлено законодавчо, передусім це стосується керівників банків.

Погодження кандидатури умовно поділяється на чотири частини:

1) співбесіда з менеджером з персоналу (за можливості водночас проводиться психологічна оцінка претендента);

2) співбесіда з особою, що перевіряє кваліфікацію претендента;

3) перевірка службою безпеки відомостей, наданих претендентом;

4) погодження кандидатури з відповідальним керівником банківської установи.

Всі свої враження кадровик викладає у письмовому висновку.

Перевіряються також причини, які спонукали особу змінити місце роботи. Може бути цікавою також оцінка його ставлення до попередніх місць роботи.

Кадровик оцінює мотивацію людини, що спонукало кандидата шукати роботу саме в цій банківській установі, про бачення своєї діяльності на новому робочому місці та цілі, які він прагне реалізувати, бажаний рівень заробітної плати і готовність підвищувати свою кваліфікацію.

Оскільки робота в банку пов'язана з обслуговуванням грошових цінностей після бесіди потрібно з'ясувати питання щодо наявності психічних захворювань, шкідливих звичок, судимостей (претенденти на посаду керівника банку повинні надати довідку з органів МВС про їх відсутність).

Слід мати на увазі, що ст. 25 Кодексу законів про працю України заборонено вимагати від осіб, які поступають на роботу, відомості про їхню партійну і національну приналежність, походження, прописку та документи, подання яких не передбачено законодавством. Згідно із ст. 24 Кодексу при укладенні трудового договору громадянин повинен подати паспорт або інший документ, що посвідчує особу, трудову книжку, а у випадках, передбачених законодавством, – документ про освіту (спеціальність, кваліфікацію), про стан здоров'я та інші документи.

Від деяких категорій працівників окремі банки вимагають рекомендації (не менше трьох) тощо.

Для запобігання можливим скаргам про порушення прав людини під час прийому на роботу кадровому менеджеру доцільно було б отримати письмову заявку претендента про те, що він добровільно погоджується відповідати на питання, які стосуються його особистого життя.

Необхідно пам'ятати, що до певних посад Національним банком України сформовані жорсткі вимоги стосовно стажу, освіти, ділової репутації, як наприклад, до керівників банків і банківських філій, касирів валютних кас, спеціалістів по роботі з банківськими металами тощо. Обов'язком керівника є перевірка відповідності кандидатів цим вимогам.

В окремих банках роблять аудіо- та відеозйомку співбесіди, про що кандидата попереджають, для подальшої перевірки правильності висновків. Зазвичай цим методом користуються у разі прийому на роботу працівників, які претендують на особливо відповідальні пости у банку. Інформація, отримана в результаті записів, придатна лише для внутрішнього використання й не може бути в подальшому оприлюднена.

Після проведення співбесіди менеджер з персоналу повинен отримати письмову згоду кандидата щодо перевірки службою безпеки наданих ним відомостей.

На другому етапі перевіряється рівень кваліфікації. Для перевірки знань та навичок претендента розробляють професійний тест, де ставляться теоретичні запитання та моделюються практичні ситуації у вигляді завдань.

Загальний культурний та професійний рівень претендента оцінюється у вільній бесіді на теми професії, в обговоренні публікацій у діловій пресі, акцентуючи увагу на знайомстві претендента з електронною поштою Нацбанку, найактуальнішими проблемами банківської системи.

Ці два етапи стосуються в першу чергу керівників середньої ланки та рядових співробітників банку. Для оцінки претендентів на посаду керівників банку існує інститут рекомендацій, аналізується досвід їх попередньої роботи на керівних посадах. Крім того, прийом на роботу представників цієї категорії узгоджується з Національним банком, який перевіряє їх відповідність посаді, вони проходять низку співбесід з керівниками регіонального управління Нацбанку та керівниками його структурних підрозділів.

Працівник служби безпеки перевіряє справжність наданих документів, проводить їх експертизу. У випадку, коли виникають сумніви, він може зробити запит про справжність документа до органу, який його видав. Перевіряються відомості, наведені в резюме кандидата та (або) його анкеті. Якщо відомості не можуть бути підтверджені документально, ця інформація перевіряється у відповідних установах та закладах. Відомості звіряються із записами у трудовій книжці.

Особлива увага надається причинам звільнення кандидата з попередніх місць роботи та термінам, протягом яких він працював. Якщо спеціаліст пішов з роботи не закривши справи, у період найбільш напруженої праці, забрала зі своїм звільненням клієнтську базу колишнього роботодавця, то банк не застрахований від повторення такого вчинку.

Також звертається увага на здатність людини зберігати конфіденційну інформацію та банківську таємницю.

Всі надані кандидатом документи, анкети та записи його співбесід передаються на перевірку службі безпеки банку. Тут ще раз слід нагадати про те, що займатись оперативною та розшуковою діяльністю можуть лише уповноважені підрозділи відповідних органів держави. Збір інформації про громадянина без його згоди є незаконним. Для того, щоб діяти в межах правового поля необхідно отримати його згоду на перевірку всіх наданих ним відомостей у письмовому вигляді.

Інформація, отримана під час перевірки рекомендацій, фіксується у письмовому вигляді. Якщо наданих відомостей недостатньо або вони не піддаються перевірці, запитуються додаткові рекомендації від кандидата.

Зараховується до штату банку кандидат після повної перевірки. Керівник служби безпеки банку готує висновок та додає його до зібраних документів.

Після розгляду наданої інформації та в разі потреби у, зустрічі з кандидатом, керівник вирішує, чи брати його на роботу.

У процесі вивчення кандидата може застосовуватись метод лайдетекції. Деякі банки мають «детектор брехні» (поліграф) та використовують його при прийомі на роботу працівника. Слід зауважити, що використання поліграфа не передбачено чинним законодавством України, тому зобов'язати кандидата пройти таку перевірку неможливо. Її можна провести лише в разі його добровільної згоди. Крім того, слід пам'ятати, що поліграф лише реєструє інформацію про стан людини в момент відповіді на поставлене запитання. Для використання поліграфа треба мати досвідченого поліграфолога, без якого достовірних даних одержати неможливо.

Відомо, що якість послуг, які надаються, та безпека клієнтів залежать насамперед від банківських службовців, які мають певні обмеження щодо їх праці.

Трудові правовідносини в банківській системі мають свої певні особливості, що випливають із специфіки діяльності банків та жорсткої регламентації їх діяльності. Ці особливості розглянуто М. Коваленко [100].

Згідно із законодавством України встановлюються вимоги щодо трудових відносин між банками та банківськими працівниками, які умовно автором поділяються на дві основні групи:

– щодо керівників банку;

– щодо посад, які пов'язані з певними специфічними видами банківської діяльності, на які банк отримує письмовий дозвіл [100, с. 41].

Керівниками банку мають бути дієздатні (дієздатність виникає з настанням повноліття, тобто з 18 років) фізичні особи, які відповідають таким вимогам:

– наявність вищої економічної, юридичної освіти чи освіти у галузі управління залежно від обійманої посади (крім членів спостережної ради);

– стаж роботи у банківській системі за відповідним фахом не менше трьох років (крім членів спостережної ради);

– бездоганна ділова репутація.

Голова правління та головний бухгалтер повинні мати попередній досвід керівної роботи у банках (не менше ніж один рік).

Не можуть бути керівниками банку особи, зазначені у статті 23 Закону України «Про господарські товариства», а саме члени Кабінету Міністрів, керівники центральних та інших органів виконавчої влади, військовослужбовці, посадові особи органів прокуратури, суду, державної

безпеки, внутрішніх справ, державного нотаріату, а також посадові особи органів державної влади, крім випадків, коли вони презентують державу в органах управління банку, особи, яким суд заборонив займатися відповідною діяльністю, які мають непогашену судимість за крадіжки, хабарництво або інші корисливі злочини. Національним банком додатково визначається, що не можуть бути призначені на керівні посади особи, які не мають бездоганної ділової репутації, професійні та управлінські здібності яких не відповідають вимогам закону тощо.

До складу правління банку повинно входити щонайменше три особи, які відповідають наведеним вимогам. Це є обов'язковою умовою для надання банку банківської ліцензії.

Підставою для зарахування на посаду голови правління та головного бухгалтера банку є рішення загальних зборів або спостережної ради (залежно від того, що саме передбачено статутом банку), але заступають на посаду вони після надання на це письмової згоди Національного банку України.

Керівниками банку можуть бути іноземні громадяни, але для їх погодження служба кадрів повинна подати відомості про наявність економічної освіти (не нижче ступеня магістра), стаж роботи та інформацію органу відповідної держави, який здійснює контроль за банківською діяльністю у банку, де працював кандидат, про відсутність у його роботі правопорушень. Крім того, у такому випадку надаються документи, що підтверджують законність перебування іноземця на території України (дозвіл на працевлаштування).

Порівняно із загальними нормами трудового права в банківських нормативно-правових актах передбачена можливість за ініціативою контролюючого органу – Національного банку – відсторонити посадову особу банку від посади у разі грубого чи систематичного порушення нею Закону про банки або нормативно-правових актів Нацбанку. Підстави для застосування цієї процедури наведено у ст. 10.1. глави 10 Положення про вживання Національним банком України заходів впливу за порушення банківського законодавства, затвердженого Постановою Правління Національного банку України від 28 серпня 2001 р. № 369. До посадових осіб, яких Національний банк має право відсторонити від посади, належать перші керівники банку та керівники філій. Рішення про відсторонення посадових осіб приймається на засіданні Комісії Національного банку.

Поряд зі звичайними підставами, працівників-керівників банку може бути звільнено за вимогою (розпорядженням) Національного банку у двох випадках: відповідно до ст. 60 Закону України «Про Національний банк України» – в разі невідповідності осіб встановленим вимогам для зайняття

зазначених посад, та згідно зі ст. 73 Закону України «Про банки та банківську діяльність» – у разі, якщо керівникові банку пред'явлено обвинувачення у вчиненні злочину, одночасно має місце порушення вимог Закону про банки або нормативно-правових актів НБУ; якщо керівника визнано винним у вчиненні корисливого злочину із призначенням покарання без позбавлення волі.

Крім вимог, які висуваються до керівників банків, є перелік посад, на які можна зарахувати лише особу, що відповідає певним вимогам контролюючого органу (керівників відділень, служби внутрішнього аудиту).

Існують певні вимоги до спеціалістів підрозділів банку, які випливають із функцій цих підрозділів.

Банки можуть не обмежуватися вимогами до своїх працівників, які встановлені законодавчо. Для підвищення рівня конкурентоспроможності, банками встановлюються додаткові вимоги до своїх службовців. Такі вимоги викладають у положеннях про відповідні підрозділи, посадових інструкціях тощо.

Зокрема, для юридичної служби основним завданням є юридичне супроводження банківської діяльності, надання консультаційних послуг, розробка та погодження договорів, представництво у судах. Крім того, банк – це не лише фінансова установа, а й юридична особи, а його не банківська господарська діяльність потребує юридичного супроводження. Вимагають обслуговування корпоративних інтересів банку в проведенні зборів акціонерів, розробці його установчих документів.

Одним з найважливіших підрозділів, без наявності якого ризикована діяльність банку підвищується, є служба безпеки банку. Служба безпеки покликана забезпечити охорону інтересів своєї установи в самому широкому розумінні цього слова. Це включає як організацію фактичної охорони банку, так і забезпечення економічної безпеки. До функцій служби безпеки відноситься перевірка відомостей, які надходять до банку. Це спричиняє необхідність вимагати від працівників служби наявності можливості для такої перевірки. Крім того, дуже важливою є участь працівників служби безпеки у кредитній діяльності банків, у перевірці документів, які надаються позичальником, перевірка його репутації, кредитної історії, наявності та фактичного стану забезпечення, яке ним пропонується, платоспроможності позичальника та/або його поручителя, супроводження кредиту, нагляд за його цільовим використанням тощо.

Контролюючі органи перевіряють відповідність певної категорії працівників посаді, яку він обіймає, а в разі виявлення такої невідповідності банк постає перед складною проблемою звільнення такого працівника, яке ним може бути оскаржено, що нерідко тягне за собою судові розгляди.

До особливостей функціонування банківських установ, які зумовлюють специфіку трудових правовідносин між банком та працівником, відноситься також те, що в процесі діяльності останні мають допуск до банківської таємниці. Розголошення таких відомостей може завдати матеріальних та моральних збитків клієнту.

Службовці банку при вступі на посаду мають підписувати зобов'язання щодо збереження банківської таємниці. Вони попереджаються про особисту відповідальність за розголошення банківської та комерційної таємниці відповідно до статей 231 і 232 КК України – про відповідальність за незаконне збирання та розголошення комерційної таємниці, ст. 164–11 КпАП України – щодо незаконного розголошення або використання інформації, що становить банківську таємницю.

Кадровий потенціал банків ще не відповідає повною мірою сучасним вимогам з об'єктивних причин. Як зазначають експерти, для належної підготовки банківського службовця, набуття мінімального практичного досвіду потрібно майже 10 років [65,с. 8].

Аналіз повідомлень засобів масової інформації й оперативних зведень правоохоронних органів про кримінальні і та диверсійно-терористичні акти проти комерційних структур дозволяє зробити однозначний висновок про високий ступінь поінформованості злочинців щодо режиму дня і динаміки діяльності підприємців – жертв, як правило, незмінно зустрічали в районі проживання чи місця роботи або з великою точністю за часом і місцем, перехоплювали на трасі. Завчасно також вивчались основні та запасні маршрути переміщення комерсантів. Злочинці мали докладні відомості про склад сім'ї, родичів, марки і номерні знаки особистих та службових автомашин, сусідів тощо, майбутніх жертв.

Невід'ємною складовою будь-якої планової злочинної акції є збір інформації. Можна виділити такі основні методи, що використовуються зловмисниками для добування відомостей про комерційні структури:

– спостереження, зокрема за допомогою мобільних і стаціонарних оптико-технічних засобів, приховане фотографування, відеозапис; вивідування інформації;

– проведення опитування, інтерв'ювання, анкетування, «спрямованих» бесід тощо;

– викрадення, приховане копіювання, підробка будь-яких внутрішніх документів особами, котрі погодилися чи були змушені здійснювати зазначені дії в корисливих цілях або у результаті погроз;

– перехоплення інформації на різних частотних каналах внутрішнього й зовнішнього радіо- і телевізійного зв'язку комерційних структур;

– технічними засобами шляхом використання різних джерел сигналів у приміщеннях комерційних структур як пов'язаних з функціонуючою

апаратурою (персональні комп'ютери), так і через спеціально впроваджену техніку негласного знімання інформації (спецзакладки, у тому числі дистанційного управління);

– за допомогою застосування системи аналітичних методів (структурний аналіз, фінансовий аналіз, аналіз собівартості продукції, аналіз науково-технічних зразків, оцінка кваліфікаційних особливостей робітників та службовців, вивчення основних матеріальних фондів тощо).

При всьому різноманітті та безсумнівних достоїнствах перерахованих вище методів усе-таки використання співробітників комерційних структур як джерела внутрішньої інформації розглядається як найбільш надійний, швидкий і ефективний спосіб одержання конфіденційних даних.

Крім того, агентурні інформаційні джерела сьогодні все активніше і наполегливо використовуються для вигідного кримінальним структурам та конкурентам впливу на стратегію і тактику поведінки керівників відповідних комерційних підприємств, а також для впливу на позицію осіб, що приймають відповідальні рішення в сфері оподатковування, митної політики, експортно-імпортних квот тощо [185, с. 268].

За даними Datapro Information Services Group [186] 81,7% порушень вчиняються самими службовцями організації, що мають доступ до її системи, і тільки 17,3% порушень вчиняються сторонніми особами (1% належить випадковим особам). За іншими даними, фізичне руйнування спричиняє близько 25% порушень (пожежа, повінь, псування) і тільки 1-2% складають порушення з боку сторонніх осіб. На долю службовців, таким чином, залишається 73-74% усіх злочинів. Відрізняючись лише цифрами, результати обох досліджень свідчать про одне: головне джерело порушень – усередині самої АСОІБ. І висновок звідси також однозначний: не має значення чи є в АСОІБ зв'язки із зовнішнім світом і чи є зовнішній захист, але внутрішній захист повинен бути обов'язково.

Можна виділити чотири основні причини порушень: безвідповідальність, самоствердження, помста і корисливий інтерес користувачів (персоналу) АСОІБ. Таким чином, для організації надійного захисту слід чітко знати, від яких саме порушень важливіше всього позбутися. Для захисту від порушень, викликаних недбалістю, потрібен мінімальний захист, для захисту від зондування системи – більш жорсткий, разом з постійним контролем – від проникнення. Метою таких дій має слугувати одне – забезпечення працездатності АСОІБ у цілому, і її системи захисту зокрема.

Причини, що спонукали користувача вчинити порушення чи навіть злочин, можуть бути зовсім різними. Близько 86% порушень становлять ненавмисні помилки, викликані недбалістю, недостатньою компетентністю, безвідповідальністю тощо. Але не це є основною загрозою для

системи. Набагато серйознішим може бути збиток, завданий у результаті навмисного впливу через образу, невдоволення своїм службовим чи матеріальним становищем, за вказівкою інших осіб. Причому збиток цей буде тим більшим, чим вище становище користувача в службовій ієрархії. Це тільки деякі з можливих причин, що спонукають користувачів йти на порушення правил роботи із системою.

Способи для запобігання порушень випливають із природи спонукальних мотивів – це відповідна підготовка користувачів, а також підтримка здорового робочого клімату в колективі, підбір персоналу, своєчасне виявлення потенційних зловмисників і уживання відповідних заходів. Перший з них – завдання адміністрації системи, другий – психолога і всього колективу в цілому. Тільки у випадку об'єднання цих заходів з'являється можливість не виправляти порушення і не розслідувати злочини, а запобігати причині їх виникнення.

При створенні моделі порушника й оцінці ризику втрат від дій персоналу необхідно диференціювати всіх співробітників за можливостями їхнього доступу до системи. Наприклад, оператор чи програміст автоматизованої банківської системи може заподіяти незрівнянно більший збиток, ніж звичайний користувач, тим більше непрофесіонал.

Так, поступово набувають великої значимості рекомендаційні листи, наукові методи перевірки на профпридатність та різного роду тестування, які здійснюють кадрові підрозділи, співробітники служб безпеки і груп психологічної підтримки, що створені в деяких банках, або з цією метою залучають сторонніх експертів.

Незважаючи на деякі позитивні приклади, в цілому доводиться, на жаль, констатувати той факт, що керівники окремих банків ще не повною мірою усвідомили необхідність організації комплексного захисту своїх структур від караних та економічних злочинів і в зв'язку з цим потребу постійного удосконалювання процесу підбору і розміщення кадрів.

Як свідчить сучасний досвід, безпека економічної діяльності будь-якого банку багато в чому залежить від того, який ступінь кваліфікації мають її співробітники, чи їхні моральні якості відповідають завданням, що розв'язуються.

Якщо об'єктивно оцінювати існуючі сьогодні процедури добору кадрів, то виявляється, що в багатьох банках і фірмах акцент, на жаль, робиться насамперед на з'ясуванні лише рівня професійної підготовки кандидатів на роботу. За такого підходу очевидно, що кадрові підрозділи виходять із застарілої концепції обмеженої матеріально-фінансової відповідальності окремих працівників за кінцеві результати своєї діяльності і схоронність конфіденційної інформації.

У сучасних же комерційних банках при дуже обмеженій чисельності співробітників, стрімко збільшуються потоки інформації й управлінських

команд, кожен співробітник стає носієм конфіденційних зведень, що можуть становити інтерес як для конкурентів, так і кримінальних співтовариств. За таких умов істотно підвищуються і змінюються вимоги до особистих та ділових якостей співробітників, а отже, і до кандидатів на роботу. Зазначена обставина спонукає керівників банків частіше звертатися до методів та процедур наукової психології, за допомогою яких можна досить швидко, надійно і всебічно оцінити можливого кандидата і скласти його психологічний портрет.

Сьогодні провідні банківські структури мають, як правило, розроблені й затверджені керівництвом організаційні структури і функції управління для кожного підрозділу. Найбільшою популярністю користуються методики складання оргсхем, на яких графічно зображується кожне робоче місце, описуються посадові обов'язки і визначаються інформаційні потоки для окремого виконавця.

За такою схемою управління та контролю ясно видно, на якій ділянці (відділ, служба, управління) потрібен фахівець відповідної кваліфікації і якою інформацією він повинен володіти для виконання функцій на своєму робочому місці. Внутрішніми розпорядженнями також визначаються вимоги до ділових і особистих якостей співробітників і обумовлюються режими збереження комерційної таємниці.

Крім того, для більшої конкретизації цих процедур на кожне робоче місце рекомендується складати професіограму, тобто перелік особистісних якостей, яким в ідеалі має відповідати потенційний співробітник. Змістовний бік і глибина розробки професіограми можуть бути різними. Це залежить у першу чергу від того, на яке робоче місце вони складаються.

Однак обов'язковими атрибутами подібних документів є розділи, що відображають професійно значимі якості (психологічні характеристики, властивості особистості, без яких неможливе виконання основних функціональних обов'язків), а також протипоказання (особистісні якості, що унеможливлюють зарахування кандидата на конкретну посаду). У деяких випадках слід не тільки вказувати професійно значимі якості, але й оцінювати ступінь їхньої виразності, тобто сформованості.

Після розробки схем управління і складання професіограм можна приступати до співбесід і застосовувати різноманітні процедури добору кандидатів на роботу.

Проблема полягає в тому, що навіть дуже досвідчені працівники кадрових підрозділів не завжди можуть правильно, достовірно і швидко оцінити справжній психічний стан осіб, які прийшли на співбесіду. Причинами тому – підвищене хвилювання, схильність окремих кандидатів до упереджених оцінок характеру діяльності деяких комерційних структур, і особливо, широке і найчастіше безконтрольне самолікування різних

психосоматичних розладів з використанням у певних випадках дуже сильних психотропних препаратів. У зв'язку з цим комерційні банки часто вимагають від кандидатів надання довідок про стан здоров'я.

З позиції забезпечення стратегічних інтересів банку є обов'язковими такі функції служби безпеки:

– визначення ступеня імовірності формування в кандидата злочинних нахилів у випадках виникнення сприятливих обставин (персональне розпорядження кредитно-фінансовими ресурсами, можливість контролю за рухом наявних засобів і цінних паперів, доступ до матеріально-технічних цінностей, робота з конфіденційною інформацією тощо);

– виявлення злочинних нахилів, що мали місце раніше, судимостей, зв'язків із кримінальним середовищем (злочинне минуле, наявність конкретних судимостей, випадки афер, махінацій, шахрайства, розкрадань на попередньому місці роботи кандидата і встановлення або обгрунтоване судження про його можливу причетність до цих злочинних діянь).

Для отримання подібної інформації використовуються можливості різних підрозділів банківських структур, у першу чергу служби безпеки, відділу кадрів, юридичного відділу, підрозділів медичного забезпечення, а також деяких сторонніх організацій, наприклад, детективних агентств, бюро зайнятості населення, диспансерів і т.ін.

Очевидно також, що представники банківських структур повинні бути абсолютно упевнені в тому, що проводять тести, співбесіди і зустрічі саме з тими особами, які є кандидатами на роботу. Мається на увазі ретельна перевірка паспортних даних, інших документів, а також отримання фотографій, де кандидати зображені без окулярів, контактних лінз, перуки, макіяжу.

Рекомендується наполягати на отриманні набору кольорових фотографій кандидата, що можуть бути використані в разі потреби для пред'явлення мешканцям за місцем його проживання, колегам по роботі.

У тому випадку, коли результати зазначених перевірок, тестів і психологічного вивчення не суперечать один одному та не містять даних, які б перешкоджали прийому на роботу певного кандидата, з ним укладається трудова угода, у більшості випадків передбачається визначений випробувальний термін (1-3 місяці).

Слід також підкреслити таку важливу обставину – особи-кандидати на відповідальні посади в банках (члени правлінь, головні бухгалтери, консультанти, начальники служб безпеки й охорони, керівники комп'ютерних центрів і цехів, помічники та секретарі перших осіб) сьогодні піддаються, як правило, стандартній перевірці, що включає:

– досить тривалі процедури збору і верифікації установочно-біографічних даних з їх подальшою аналітичною обробкою;

– подання рекомендаційних листів від відомих підприємницьких структур з подальшою їх перевіркою;

– перевірки за обліками правоохоронних органів, за місцем проживання і за попереднім місцем роботи;

– серії співбесід і тестів з подальшою психоаналітичною обробкою результатів.

Серйозний вплив на забезпечення безпеки банків мають процедури звільнення співробітників. На жаль, окремих керівників часом мало цікавлять почуття і переживання персоналу – за тих чи інших причин співробітник попадає під скорочення чи самостійно виявляє бажання залишити банк. Як показує досвід, такий підхід призводить, як правило, до серйозних негативних наслідків. Сучасні психологічні підходи до процесу звільнення дозволяють виробити таку принципову рекомендацію: які б не були причини звільнення співробітника, він повинен залишати банк без почуття образи, роздратування й помсти.

Тільки в цьому випадку можна сподіватися на те, що співробітник, котрий звільняється, не зробить необдуманих кроків і не буде використовувати комп'ютерне проникнення.

При надходженні заяви про звільнення рекомендується в усіх без винятку випадках провести зі співробітником бесіду за участю представника кадрового підрозділу і кого-небудь з керівників комерційної структури. Однак до бесіди доцільно зібрати таку інформацію про співробітника, що звільняється:

– характер його взаємин з колегами в колективі; ставлення до роботи; рівень професійної підготовки; наявність конфліктів особистого чи службового характеру;

– раніше мали місце висловлення чи побажання перейти на інше місце роботи;

– доступ до інформації, у тому числі такої, що складає комерційну таємницю.

При мотивації звільнення доцільно, як правило, утримуватися від посилань на негативні ділові й особисті якості співробітника. Після оголошення про звільнення рекомендується уважно вислуховувати контрдокази, аргументи і зауваження співробітника щодо характеру роботи, стилю керівництва банком і т.ін. Якщо підходити не упереджено й об'єктивно до подібної критики, то ці висловлювання можуть бути використані надалі дуже ефективно в інтересах самого банку. У ряді випадків співробітнику, що звільняється, цілком серйозно пропонують навіть викласти на письмі свої рекомендації, звичайно, за відповідну винагороду. При остаточному розрахунку рекомендується, незалежно від особистісних характеристик співробітників, які звільняються, брати в них підписку про нерозголошення конфіденційних відомостей, що стали відомими в процесі роботи.

Крім того, у найбільш гострих і конфліктних ситуаціях звільнення персоналу проводяться оперативні профілактичні заходи щодо нового місця роботи, проживання, а також в оточенні носіїв комерційних секретів.

Персонал робить істотний, а в більшості випадків навіть вирішальний вплив на інформаційну безпеку банку. У зв'язку з цим підбір кадрів, їхнє вивчення, розміщення і кваліфіковано проведене звільнення значною мірою підвищують стійкість комерційних підприємств до можливого стороннього негативного впливу й проникнення протиправних елементів. Регулярне вивчення всіх категорій персоналу, розуміння об'єктивних потреб співробітників, їхніх інтересів, справжніх мотивів поведінки та вибір відповідних методів об'єднання окремих індивідуумів у працездатний колектив – усе це дозволяє керівникам успішно вирішувати складні виробничі і комерційно-фінансові завдання, у тому числі пов'язані із забезпеченням економічної безпеки.

Узагальнюючи основні рекомендації, думається, що програма роботи з персоналом у комерційній структурі могла б мати такий вигляд:

– добування в межах чинного законодавства максимального обсягу відомостей про кандидатів на роботу, ретельна перевірка поданих документів як через офіційні, так і оперативні можливості, зокрема, служби безпеки банку чи детективного агентства, системність в аналізі інформації, зібраної про відповідну кандидатуру;

– проведення комплексу перевірочних заходів щодо кандидатів на роботу, їхніх родичів, товаришів по службі, найближчого оточення в тих випадках, коли розглядається питання про прийом на керівні посади чи допуск до інформації, що складає банківську таємницю;

– використання сучасних методів вивчення особи, зокрема співбесід і тестувань, для створення психологічного портрета кандидатів на роботу, який би дозволяв упевнено судити про основні риси характеру і прогнозувати ймовірні дії в різних екстремальних ситуаціях;

– оцінка з використанням сучасних психологічних методів різнопланових факторів, що, можливо, перешкоджають прийому кандидатів на роботу чи їхньому використанню на конкретних посадах;

– визначення для кандидатів на роботу в банках деякого іспитового терміну з метою подальшої перевірки і виявлення ділових та особистих якостей, інших факторів, які б могли перешкоджати зарахуванню на посаду;

– введення в практику регулярних і несподіваних комплексних перевірок персоналу, у тому числі через можливості служб безпеки;

– навчання співробітників кадрових підрозділів і служб безпеки сучасним психологічним підходам до роботи з персоналом, соціальним, психоаналітичним, етико-моральним методам, навичкам використання сучасних технічних засобів для фіксування результатів інтерв'ю і співбесід,

прийомам проведення цільових бесід «втемну» і процедурам інформаційно-аналітичної роботи з документами кандидатів;

– призначення з числа перших керівників банківських структур куратора кадрової роботи для проведення контролю за діяльністю кадрових підрозділів і служб безпеки при роботі з персоналом.

Поряд з іншими причинами, відсутність досвіду зумовила й те, що із 157 комерційних банків, які функціонували у 2002 р. в Україні, 11 спрацювали зі збитками, а чистий прибуток ще 14 банків коливався в межах від 7 до 99 тис.грн. Рентабельність активів банків України на початок 2003 р. становила лише 1,3%.

Нерідко в банках злочинні дії допускають їх керівники. Так, у травні 2003 р. Печерський місцевий суд Києва виніс вирок колишньому першому заступнику Національного банку України В.Бондарю, засудивши його до 5 років позбавлення волі. Йому інкриміновано зловживання службовим становищем і нанесення державі збитків на суму близько 20 млн доларів. Він заключив в 1997 р. контракт від імені НБУ із банком Credit Swiss First Boston (Швейцарія і Кіпр) про перерахування зазначених валютних коштів. Після перерахування вони осіли в офшорних банках і в Україну не повернулись.

Внаслідок злочинної кредитної політики збанкрутував акціонерно-комерційний банк розвитку агропромислового комплексу «Україна», який входив у першу групу найпотужніших банків України. До його краху причетні високі посадові особи держави, про що повідомлялось у пресі («Факти», № 231 від 18 грудня 2001 р.). Свідомо чи підсвідомо вони зіграли на руку зарубіжним конкурентам банку в галузі агропромислового комплексу. Цьому також активно сприяло «організоване злочинне угрупування, що діяло у банківській сфері».

За даними тимчасової слідчої комісії ВР із з'ясування причин банкрутства банку «Україна», обсяги прострочених і неповернутих кредитів, одержаних суб'єктами підприємницької діяльності в банку «Україна», за рахунок відсотків збільшилися з 1,3 до1,45 млрд грн. За півтора року здійснення ліквідаційної процедури повернуто лише 52 млн грн, причому жодний з найбільших боржників не скоротив свого боргу.

Водночас банк мав близько 2600 боржників, які своєчасно не повернули надані їм кредити на суму 797 млн грн і заборгували за відсотками 650 млн грн. Тобто борги перед банком становили майже 1,5 млрд грн [174, с. 9].

Для координації зусиль у розв'язанні спільних завдань в столиці України утворено Київський Банківський Союз (КБС), президентом якого обрано Л.Черновецького. Обрано колегіальний орган – Спостережну раду. Лише у 2002 р. КБС порушено близько 90 питань та ініційовано розгляд понад 20 справ у судових органах задля захисту прав та інтересів банку.

«Якщо раніше, – коментує Леонід Чеповецький, – ми займалися захистом прав та законних інтересів банківських установ у судовому порядку, на законодавчому рівні та шляхом постійних переговорів і консультацій з державними органами влади, то зараз плануємо розпочати такі важливі форми роботи, як створення кредитного бюро, комплексних банківських рейтингів, цільових фондів. Із нами готові співробітничати банківські асоціації різних країн світу. Цим потрібно постійно займатися.

Крім того, кількість банків – членів КБС зросла, зросла й кількість пропозицій з удосконалення законодавства, врегулювання проблем, що виникають у роботі банків» [97, с. 27].

Банкам України, які все більше набувають ознак корпоративності, сьогодні доводиться працювати у важких соціально-економічних умовах. Так, у співдоповіді голови Комітету Верховної Ради України з питань національної безпеки і оборони Георгія Крючкова «Демографічна криза в Україні: причини і наслідки» на парламентських слуханнях 21 травня 2003 р., зазначається: що 40 млн громадян України, як зазначено в минулорічному Посланні Президента, перебувають за межею бідності, тобто мають дохід нижче прожиткового мінімуму, а 7,9 млн – злиденні; за рівнем безробіття Україна посідає одне з перших місць в Європі; що обсяг валового внутрішнього продукту на душу населення в нашій країні, за даними зарубіжних аналітиків, у 30 разів нижчий, ніж у середньому по Європейському союзу, і в більш як три рази нижчий за середньосвітовий показник (з урахуванням країн Америки, Азії, Латинської Америки).

У десятків мільйонів громадян на харчування витрачається практично весь заробіток. І це при тому, що населення України споживає, за даними, які наводились у пресі, хліба на 20%, молока – удвічі, цукру – в два з половиною рази менше, ніж це потрібно за біологічними нормативами.

Рік у рік зростає тягар витрат населення на освіту й охорону здоров'я, які всупереч Конституції фактично стали платними і недоступними для бідних людей [82, с. 8].

Як доводить директор Інституту прогнозування НАН України, академік В. Гаєць [72, с. 10–11], виходячи із огляду основних геоекономічних подій, що відбулись останнім часом, можна дійти висновку: існуюча нині світова система розподілу праці несприятлива для України. У наших найближчих сусідів на Заході справи в економіці не настільки блискучі, як багато кому здається. У більшості з них від'ємні торговельні баланси, тобто вони купують більше, ніж продають.

Україні давно треба було б перейти від екзогенних (зовнішніх) факторів розвитку до ендогенних (внутрішніх). Звичайно, при цьому слід всіляко підтримувати вигідну для країни зовнішню торгівлю. Але вже ні в кого не

викликає сумнівів потреба у розширенні та поглибленні внутрішнього ринку, котрий і має освоїти значну частину наявних у країні ресурсів.

Дуже важким для України було ХХ століття: дві світові війни, громадянська війна, революція, голод, репресії, двічі змінювався суспільно-політичний лад. Але Україна упродовж останнього століття розвивалася, незважаючи на справді колосальні втрати, дещо вищими темпами, ніж середньосвітові [72, с. 11].

Від ресурсовидобувної схеми розвитку, що не веде вперед, ми повинні перейти до інноваційної моделі.

Не варто розраховувати також на кредити міжнародних фінансових організацій та іноземні інвестиції: по-перше, їх не вистачить, по-друге, тут не обійтися без небажаного, непередбачуваного розвитку подій. Та гроші в нашій країні є. За деякими даними, за межами країни постійно працюють близько трьох мільйонів українців. Принаймні, ці мігранти, найчастіше нелегальні, заробляють до 10 млр доларів за рік, а може, й більше. Значна частина цих коштів заощаджується й може бути інвестована в економіку України, якщо держава здобуде довіру цих людей. Та водночас, така масова міграція свідчить і про інше: в України немає часу на зволікання, інакше вона позбудеться своїх трудових ресурсів, за які теж точиться конкуренція на глобальному ринку.

І взагалі, як стверджує В. Гаєць, правильно вчинили росіяни: вони доручили визначити пріоритет галузей солідній академічній науці. Справа це надто серйозна, щоб доручати її політикам. Ми можемо йти достатньо швидко, але Україні для цього слід змінити модель розвитку.

Отже, визнані вчені вважають, що Україні слід створити власну модель розвитку, орієнтуючись на ендогенний потенціал, в т.ч. науковий. Це позбавить залежності від зовнішніх чинників, сприятиме утвердженню суверенітету, за який так довго боролись і який швидко можна втратити.

У С. Тігіпка рішення про кадрові реформи було одним з перших на посаді голови. Постанова № 16 «Про внесення змін у структуру Національного банку України» побачила світ 21 січня 2003 р.

Відповідно до документа в Нацбанкові були створені три нових департаменти – аудити, у яких залучені 33 фахівці, зовнішньоекономічних відносин – 27 осіб, організації виробництва й господарської діяльності, що нараховує 7 осіб. Департамент особисто-грошового звернення доповнений 11 фахівцями, з яких сформують управління експертизи, захисту грошей і нумізматики. Також реформовано прес-службу, її розширили до управління зв'язків із громадськістю і ЗМІ, що складається з 8 осіб. З'явилася в НБУ і наукова кузня: створена група, що зайнялася організацією науково-дослідного інституту в структурі Центробанку.

Поряд з цими масштабними новаціями планувалося велике скорочення кадрів. Зокрема, скасований відділ з питань роботи з програми МВФ департаменту монетарної політики. Його функції передані департаменту зовнішньоекономічних зв'язків. Скорочена кількість співробітників у департаменті внутрішнього аудиту, управлінні будівництва і реконструкції, управлінні організації виробництва, експертизи і нумізматики департаменту готівково-грошового обороту.

У головному банку такі перестановки пояснили потребою у кадрових реформах, «виходячи з принципу: щоб організація нормально працювала, як мінімум, раз у два роки необхідно цілком або частково змінювати основні напрямки й загальну структуру. Процеси рухаються в економіці, державі та й у самому Національному банку. Під нові завдання формується нова структура. Я вважаю, що питання кадрових перестановок не має значення для банківської системи в цілому, не слід орієнтуватися на персоналії. Варто орієнтуватися на структуру, її основний напрямок роботи», – відзначив в інтерв'ю «Діловій столиці» 27 січня 2003 р. заступник голови НБУ А. Яценюк.

Вітчизняний банківський менеджмент має враховувати зарубіжний досвід, багатий своєю історією і практикою спробував вивчити банківський менеджмент провідних країн світу в 2000 р. здійснив російський автор Е. Старобинський [156]. Результати свідчать, що в США кредитно-фінансова система значно молодша аналогічних систем Європи. Для американського банківського менеджменту є характерним навчання банківських службовців за різними програмами, що призводить іноді до непогодженостей у практичній діяльності банків. Підвищена увага служб з роботи з персоналом до питань тестування, що не завжди представляє об'єктивні характеристики кандидатів на вакансії, які відкрилися. Підбір вищих керівників банку з боку інших кредитно-фінансових структур. Підвищена плинність кадрів, що досягає 20-25% на рік, неефективна робота з резервом на висування. Недостатня увага до питань підвищення кваліфікації банківських службовців, відсутні спеціалізовані навчальні програми для цих цілей. Контрактна система з обмеженням, порівняно з Європою, зайнятості на 3-4 роки. Широко практикується система соціальних пільг, адекватна за вартістю 60-65% річному доходу банківських службовців.

Багато банків США мають у своєму штаті професійних операторів поліграфа, що забезпечують деякою мірою реалізацію програм щодо кадрів і безпеки. Завдяки цьому показник виявлення за допомогою поліграфа приховання фактів судимості при найманні на роботу в банківські установи і ювелірні магазини склав 95%. Поліграф дозволяє з'ясувати, чи не займався кандидат шахрайством і розкраданням на попередніх роботах, чи немає в

нього зв'язків зі злочинцями, чи не упроваджувався він у дану структуру конкурентами або злочинними угрупованнями.

В Японії підбирають кадри банків і керують ними значно ефективніше, ніж це відбувається в європейських банках та банках США. Продуктивність праці в банках США, керованих японцями, вища на 30-40%, ніж у банках, де менеджери – американці.

Для банківського менеджменту в Японії властива наявність у штаті банків фахівця з менеджменту. Ефективно діючі фірми, що консультують діяльність банків у сфері фінансів і менеджменту. Відбір майбутніх працівників банку ведеться на перших курсах спеціалізованих навчальних закладів. Кандидати на роботу в банки додатково слухають лекції практиків з числа керівного складу банків. Банк для перспективних студентів виділяє додаткові кошти для повної чи часткової оплати навчання і підвищених стипендій. Система «довічного наймання», яка використовується в банках, гарантує постійне підвищення заробітної плати й одержання різних соціальних пільг залежно від вислуги років. Підвищується кваліфікація співробітників здійснюється у спеціалізованих навчальних центрах з відривом від роботи. Широко практикується система моральних заохочень співробітників, застосовується рангова система просування по службі. Використовуються методи самооцінки співробітниками своєї роботи паралельно з оцінками, що даються менеджерами. Постійно практикується горизонтальне переміщення працівників, що сприяє вивченню суміжних професій. Регулярно проводяться семінари і конференції для менеджерів банків. У штатах банків передбачені посади так званих хрещених батьків – досвідчених менеджерів, які наставляють молодих співробітників протягом кількох років.

Банківська система ФРН широко відома сполученням фінансово-кредитних організацій і збереженням традицій у менеджменті. Більшість фінансово-кредитних організацій сформовано на основі однакових принципів. Становить інтерес злиття банків ГДР і ФРН наприкінці 80-х і початку 90-х років.

Постійної уваги надається перепідготовці працівників служб персоналу за спеціальними програмами. Організовано стажування слухачів у кращих банках країни і за рубежем. Провадиться постійна перепідготовка різних категорій персоналу, проводяться тренінги на суміжних посадах. Висококваліфіковані куратори опікують молодь. Використовуються різні види оплати праці залежно від рівня кваліфікації, досвіду, оволодіння новими методами роботи, знання іноземних мов тощо.

У банках Франції до рівня підготовки персоналу пред'являються підвищені вимоги, викликані наявністю твердої конкуренції. Підвищені витрати на підготовку персоналу (до 12% проти 5-6% у США).

Координуюча роль належить Центральному банку Франції, що виражається в розробці методології процесів фінансово-кредитної системи і персонального менеджменту. Використовуються конкурси при заміщенні різних посад. Існує тісний зв'язок просування по службі з перепідготовкою і підвищенням рівня знань.

Здійснюється навчання всіх банківських службовців за програмою «Психологія спілкування». Висока питома вага менеджерів і фахівців – жінок (до 20%). Проводиться постійне інформування персоналу про діяльність банку за зазначені періоди, про вакансії, що відкрилися, і про використовувані елементи кадрової політики.

У Франції існує центр підготовки і перепідготовки банківських службовців.

В італійських банках на півночі країни використовуються американські методи управління персоналом.

У південних районах з чисто італійською специфікою управління в банках провадиться без визначеної системи. В Італії практично «радянська» система підбору і переміщення кадрів на основі суб'єктивних факторів: родинних і дружніх зв'язків і т.п. Відсутні стимули, що сприяють підвищенню кваліфікації. Віддається пріоритет адміністративним методам управління, а не методам економіко-соціального характеру.

До останнього часу в банках Росії до служб управління персоналом було традиційне відношення, таке саме, як і до інших штабних служб. І тільки кілька великих банків, на чолі яких стоять люди, що зуміли перейняти досвід найбільших банків західних країн, змінили своє відношення до діяльності служб управління персоналом. Статус працівників служби управління персоналом дуже низький. У банках західних країн керівником таких служб є віце-президенти. Високий статус керівників служб управління персоналом дозволяє останнім бути в курсі всіх справ банків.

Ми поділяємо думку Е. Старобинського, що служба управління персоналом повинна мати спеціальне положення, яке містило б: загальну частину; функціональні обов'язки; права; відповідальність. Окрім цього розробляються посадові інструкції для всіх працівників.

Положення передбачає субординацію, порядок призначення і переміщення керівників і фахівців, відповідальність, виконання функцій у просторі й часі. Служба управління персоналом, так само, як і інші підрозділи, має визначати стратегію на перспективу розвитку банку. Першочерговим завданням цієї стратегії є укомплектування штабу банку за рахунок фахівців з високою кваліфікацією.

Стратегія і тактика стосовно основного завдання містить такі головні моменти: кадрова політика повинна враховувати особливості конкретного банку, його матеріальні й організаційні можливості та провадитися всіма

менеджерами банку, а не тільки служби управління персоналом і працівниками вищого ешелону керівництва.

Кадрова політика в банках має одну дуже важливу особливість – працівник постійно повинен знаходитися під спостереженням. Важливо знати про зміни в характері, появі зв'язків, що ганьблять працівників тощо.

Для цього оформляється й ведеться індивідуальне досьє, яке закрите навіть для об'єкта, що спостерігається. У досьє заносяться дані про особисті зв'язки, поведінку, зарозумілість, прояви заздрості, захоплення жінками, схильності до спиртного, до азартних ігор, невиправдано швидке зростання добробуту і т.п. Індивідуальне досьє оформляється відразу ж після приходу співробітника в банк. Такі дані містяться в комп'ютері, який не є елементом комп'ютерної мережі банку.

У Росії прийняті на роботу в банки співробітники проходять іспитовий термін: технічний персонал – 2-3 місяці; фахівці – до 6 місяців; менеджери – 1 рік. На цій стадії приймається остаточне рішення про наймання працівника або відмову йому. Іспитовий термін повинен бути передбачений у контракті. Подібна практика дозволяє банкам вчасно скинути баласт. Великі російські банки мають зв'язок з профільними фінансово-економічними інститутами і коледжами.

Постійно розширюється сфера банківських послуг, змінюються організаційні структури в зв'язку з кон'юнктурою ринку, банк інвестує різні галузі господарства, упроваджується нова техніка, використовується Інтернет. Усе це створює передумови для постійного підвищення кваліфікації працівників. У західних країнах витрати на підвищення кваліфікації коливаються від 7 до 12% від суми заробітної плати персоналу.

Українські банки у своїй більшості не мають стратегічних планів підготовки і перепідготовки співробітників, відсутня необхідна мотивація й об'єктивна оцінка результатів роботи з персоналом, навчання.

Із викладеного випливають такі висновки.

ВИСНОВКИ ДО РОЗДІЛУ ІІІ

Важливу роль у банківській діяльності відіграють різноманітні ризики.

Банківський ризик –це певна ситуаційна характеристика діяльності банку, яка вказує на невизначеність результату та можливі небажанихі наслідки, в разі невдачі. Такими наслідками, як правило, є: неотримання прибутку, виникнення збитків, внаслідок невиплат за отриманими кредитами тощо.

За часом ризики розподіляються на ретроспективні, поточні та перспективні. За ступенем: низькі, помірні, повні. За основними факторами виникнення банківські ризики можна поділити на політичні та економічні. Під політичними

ризиками слід розуміти ризики, які зумовлені змінами політичного становища, що негативно впливає на результати діяльності підприємств.

Економічні ризики – це такі ризики, які зумовлені негативними змінами в економіці країни або самого банку. Найпоширенішим видом економічного ризику, в якому сконцентровані окремі ризики, є ризик незбалансованої ліквідності, що являє собою неможливість своєчасно виконувати платіжні зобов'язання, зміни кон'юнктури ринку, рівня управління.

Виробничий ризик – це ризик, що може виникнути на виробництві, і який слід враховувати під час складання прогнозів.

Комерційний ризик – це ризик, який треба враховувати під час визначення прогнозів, він може виникнути у процесі реалізації продукції.

Фінансовий ризик є найнебезпечнішим, оскільки його важко спрогнозувати, і включає підвищення податкових ставок посеред фінансового року чи облікової кредитної ставки; певна фінансова стратегія фірми, якщо вона змінює ціни на цінні папери; зміна Національним банком курсу валют тощо.

Усі зазначені види ризику можуть бути трьох рівнів: допустимий, критичний, катастрофічний.

До зовнішніх ризиків відносяться ризики, які не пов'язані з діяльністю банка. На їх рівень впливає велика кількість факторів – політичні, економічні, демографічні, соціальні, географічні та ін.

До внутрішніх – ризики, які зумовлені діяльністю самого банку, його клієнтів чи конкретних контрагентів. На їх рівень впливає ділова активність керівництва банку, вибір політики та тактики тощо.

Останнім часом банки більш гостро відчувають потребу в управлінні ризиками. Під управліннями ризиками, слід розуміти всі вжиті заходи, які направлені на мінімізацію відповідного ризику та пошук оптимального співвідношення прибутковості й ризику, що має включати оцінку, прогноз і страхування відповідного ризику.

Економічний валютний ризик – це ризик зміни вартості активів чи пасивів банків внаслідок майбутніх змін курсу.

Ризик переводу – це ризик зміни вартості активів і зобов'язань банку, пов'язаний зі зниженням курсу валюти.

Банки бувають державними та комерційними, які в свою чергу поділяються на спеціалізовані, галузеві та універсальні. У кожному з них присутні всі види ризиків, але вірогідність частоти їх виникнення і специфіка залежить від самого банку.

Залежно від характеру банківських операцій ризики можна поділити на ризики активних і пасивних операцій.

Банк взагалі регулює свої ресурси для активних операцій завдяки пасивним. До пасивних операцій комерційних банків відносять відрахування їх прибутку на формування та збільшення статутного капіталу; величину кредитів, отриманих від інших юридичних осіб, депозитні операції. Загалом, лише перша група пасивних операцій формує власні кошти банку, а отримання банківських позик від інших юридичних осіб необхідне, найчастіше, для оперативного регулювання ліквідності балансів банку або для видачі непередбачених кредитів.

Депозитні операції – це операції із залученням коштів юридичних і/ або фізичних осіб у вклади або до запитання, або на визначений термін. Ризики

пасивних операцій пов'язані з можливими ускладненнями в забезпеченні активних операцій ресурсами. Частіше за все це ризик, пов'язаний з ефективністю діяльності визначального вкладника (один виробник або група «споріднених» компаній).

Для попередження ризику щодо формування депозитів банкам слід дотримуватись оптимального співвідношення між пасивними і активними депозитними операціями, тобто вкладами підприємств у банк і вкладами, розміщеними одними банками в інших банках; визначати розмір і ліквідність залучених для зберігання цінних паперів для підвищення рівня та якості мобільних засобів; знайти доцільне мінімальне співвідношення власних засобів і ризикових активів; розробити методи розрахунку коефіцієнта пов'язання депозитів з обліком особливостей конкретного банку і керуватися ним при розміщенні депозитів.

Ризики активних операцій пов'язані з так званим рівнем відсотків ризику, на який банки постійно наражаються в процесі своєї діяльності, тобто небезпекою втрат внаслідок перевищення сплачених відсоткових ставок над отриманими. Підвищення відсоткових ставок призводить до падіння курсу цінних паперів із твердими відсотками, а відтак – і до знецінення банківського портфелю, завдає курсових збитків. Крім того, різниця між відсотковими доходами і витратами становить основу банківського прибутку. Різка зміна ставок у різних сегментах ринку може негативно позначитися на прибутковості операцій банку.

Управління процентним ризиком складається з управління активами (кредитами й інвестиціями) та пасивами (залученими коштами).

Аби зменшити ризик деякі банки вводять до відсоткової ставки за розміщеними коштами ризикову відсоткову ставку (договірну надбавку) або розмір страхового відсотка (коли позичку страхує сам банк). В умовах інформації, як правило, аналізують реальні та номінальні відсотки. Щоб уникнути відсоткового ризику банки активно надають кошти на тривалі строки, а для рефінансування залучають кошти на короткий термін.

Обчислюючи коефіцієнт відсткового ризику, банки враховують ускладнення, які майже завжди виникають під час погодження строків платежу банку за зобов'язаннями і отримання платежів від клієнта; ймовірність невиконання зобов'язань партнером.

Фінансові ризики можуть бути визначені таким чином: чим більше залучених коштів мають банки, акціонерні товариства, підприємства, в тому числі і спільні банки, тим вищий ризик для їх акціонерів, засновників. Водночас, залучені кошти є важливим і вигідним джерелом фінансування, тому що найчастіше обходяться дешевше, ніж випуск та продаж додаткових тиражів цінних паперів.

Системний ризик пов'язаний зі змінами цін на акції, їх доходністю, поточним і очікуваним відсотком за облігаціями, очікуваним розміром дивіденду, і додатковим прибутком, викликаним загальноринковими коливаннями. Він об'єднує ризик відсоткових ставок, ризик змін загальноринкових цін і ризик інфляції. Піддається достатньо точному прогнозу, тому що тіснота зв'язку (кореляція) між біржовим курсом акції і загальним станом ринку регулярно і достатньо достовірно реєструється різними біржовими індексами.

Несистемний ризик не залежить від стану ринку і є специфікою конкретного підприємства, банку. Він може бути галузевим та фінансовим. Основними факторами, що впливають на рівень несистемного портфельного ризику, є

наявність альтернативних сфер докладання (вкладання) фінансових ресурсів, кон'юнктура товарних і фондових ринків та ін.

Сукупність системних та несистемних ризиків називають ризиком інвестицій.

Одним з основних способів виміру рівня ризику є аналіз залежних і незалежних, зовнішніх та внутрішніх факторів, що впливають в конкретній ситуації за допомогою методів експертних оцінок.

Крім того, в практиці комерційних банків країн з розвинутою ринковою економікою широко використовується система банківських гарантій. Залежно від кількості банків, що беруть участь в гарантійних операціях, розрізняють прямі, побічні і посередницькі операції.

Для зниження рівня галузевого ризику банку необхідно обслуговувати клієнтів, що належать до різних галузей народного господарства. Таким чином, знижується рівень ризику сезонності, адже верхні і нижні точки сезонних коливань (традиційні і неочікувані) різноманітних клієнтів не співпадають, ризику інфляції, валютних ризиків, ризиків форс-мажорних обставин.

За належністю до різних видів власності виробники можуть бути поділені на такі групи: державні, приватні, кооперативні, акціонерні. Останні два види можуть бути спільними (транснаціональними) і мононаціональними. Залежно від цього різні види ризиків набувають більшої чи меншої значущості в процесі їх діяльності. Завдання банку – підібрати портфель своїх клієнтів таким чином, щоб самому мати оптимальне співвідношення між активними і пасивними операціями, зберігати рівень своєї ліквідності й рентабельності на потрібному для безперебійної діяльності рівні.

Регулювання банківського ризику базується не на оцінці фінансового становища позичальника, а на встановленні певного співвідношення між сумами виданих кредитів і власних коштів самого банку, тобто передбачається створення резервного потенціалу у банків для покриття ймовірних збитків у випадку розорення клієнтів.

Тільки від конкретної ситуації залежить, яким способом комерційні банки будуть аналізувати рівні всіх своїх ризиків і управляти ними.

Тим часом у структурні кредитних ринків розвинутих країн активно діє система спеціалізованих кредитних бюро, які відіграють важливу роль у зниженні ризиків виконуваних угод. Вони створюються для того, щоб кредитор міг одержати інформацію про стан платоспроможності позичальників, порушення ними платіжної дисципліни і на її підставі оцінити ступінь ризику майбутньої угоди. Закордонний досвід показує, що вирішити ці проблеми можна тільки за допомогою кредитних бюро, створених для обміну відомостями про прохачів позик між кредиторами. Це, з одного боку, знижує ризики здійснюваних угод, а з іншого – змушує всіх учасників ринку вкрай вимогливо ставитися до своєї кредитної історії, яка фактично є основою ділової репутації.

Незважаючи на всю специфічність українських умов, закордонний досвід розвитку кредитних бюро корисний для нашої країни. На сьогодні створенню в Україні таких структур перешкоджає відсутність спеціального закону про кредитні бюро. Якщо названий закон буде розроблено і прийнято, внаслідок якого це бюро у нас з'явиться, то кредитні ризики можуть бути значно знижені.

Ризик економічного зростання полягає, зокрема, і в політичних процесах. А тому ми зіштовхуємось із серйозними перешкодами банківського реформування.

Україна впритул підійшла до проведення політичних реформ... Нашій державі, суспільству яке лише на шляху до громадянського, вкрай необхідно структурувати політичну владу, чітко розподілити повноваження владних інституцій.

На практиці, організовуючи захист банківської системи і її діяльності, слід враховувати різні варіанти ризиків, зокрема: ретроспективні, поточні та перспективні; низькі, помірні й повні; політичні та економічні; зовнішні і внутрішні, а також – виробничі, комерційні, фінансові; допустимі, критичні, катастрофічні. Важливо їх своєчасно спрогнозувати і надійно управляти ними, уникаючи важких наслідків, не лише ризиків, але і найпоширеніших незаконних операцій, здійснюваних через банківську систему. При цьому прерогатива в боротьбі із зовнішніми ризиками надається органам влади і правоохоронної системи, а внутрішніми – НБУ і БСУ.

В умовах розвитку посттоталітарного суспільства стрімкого поширення набуває тіньова економіка як наслідок криміналізації економічних процесів. У зв'язку з цим введено термін кримінальної безпеки, яка становить такий різновид безпеки, який не має конкретного носія, але дуже впливає на економічне становище держави (економічні злочини, криміналізація суспільства тощо) та її мешканців (вбивства, грабежі, насильство, крадіжки тощо). Одним із характерних проявів криміналізації посттоталітарного суспільства є зростання частки тіньової економіки в сукупності з економічною діяльністю, зростання злочинності. Серед основних форм тіньової економіки виділяють такі: неофіційна; фіктивна; підпільна.

Незаконні операції в БСУ умовно поділяються на дві частини: ті, які застосовуються безпосередньо у банківських установах; ті, якими користуються підприємницькі структури з використанням банківських установ.

Набуло поширення розкрадання кредитів, які надаються невеликим комерційним структурам (найчастіше таким, що тільки утворилися спеціально для отримання такого кредиту) або приватним особам.

При вивченні підстав банкрутства слід звернути увагу на те, чи не є воно навмисним або псевдобанкрутством, коли боржник заявляє про свою неплатоспроможність, а сам приховує або передає за допомогою псевдоугоди чи інакше майно у володіння інших осіб. Всі такі факти та випадки фіктивної застави за підробленими або юридично неправомірними документами, або застави без її реального майнового забезпечення, – є доказами шахрайства з боку боржника. У документуванні розглянутого шахрайства є певні труднощі, які полягають у тому, що одержання кредиту і його повернення відноситься до сфери фінансових та цивільно-правових відносин, юридичний та економічний аналіз яких дуже складний, і не завжди приводить до реального наслідку – притягнення боржника до кримінальної відповідальності.

Розкрадання грошових коштів нерідко провадиться під виглядом їх конвертації у ВКВ, в тому числі з приховуванням валюти за кордоном, що продовжує залишатися одним із засобів незаконного збагачення ділків «тіньової» економіки.

При документуванні цих правопорушень велике значення має пошук підтвердження інформації про: використання отриманих грошей не за призначенням; відсутність на розрахунковому рахунку вказаної комерційної організації грошових коштів; ліквідацію офісу або подання в договорі неіснуючої адреси; розпродаж майна цієї комерційної організації або незаконне оголошення її

банкрутом; оформлення фіктивних застави, поруки або видача фіктивних векселів; подання підроблених банківських та інших документів для підтвердження «реальності» угоди; здійснення конвертації грошей комерційними організаціями, статутом яких непередбачена зазначена діяльність.

Розкрадання та привласнення грошових коштів відбувається також шляхом привласнення нарахованих відсотків за вкладами клієнтів або переказу коштів клієнтів (без їх відома) з депозитних рахунків на інші рахунки чи у фонди. Привласнення посадовими особами банку грошових коштів таким способом може відбуватися за рахунок: свідомо неправильного визначення відсотків за вкладами, частіше всього у випадках, коли на рахунку клієнта: є не «кругла» сума, а також коли грошові кошти лежать на рахунку у банку неповний календарний рік.

Збір доказів на стадії реалізації матеріалів полягає в пошуку, реєстрації, аналізі перш за все документів, які містять дані про виконання тих чи інших операцій по вкладу.

У кожному випадку виявлення зловживань, скоєних працівниками банківських установ, повинно бути організовано суцільне звірення записів в ощадних книжках вкладників із записами в їх особистих рахунках і документах, які знаходяться в бухгалтерії банку.

Значного поширення останнім часом набуло також розкрадання облігацій державної позики та інших цінних паперів при купівлі їх від населення.

Окрему групу розкрадання грошових коштів вкладників становить повне або часткове їх неоприбуткування.

Свої особливості мають незаконні операції, що вчинюються у підприємницьких структурах з використанням банківських установ. Протиправна діяльність у банківській системі в основному пов'язана із зловживаннями при оподаткуванні, наданні кредитів, позичок; конвертацією, з подальшою крадіжкою грошових коштів через «ЛОРО-рахунки»; незаконною емісією цінних паперів банків, вексельним обігом, нецільовим використанням та розкраданням бюджетних коштів, приховування. Аналітичний прогноз можливих правопорушень дає підстави вважати, що зараз, за умов первинного накопичення капіталу, ця категорія зловживань найбільш поширена та суспільно небезпечна і здатна підірвати основи економіки й остаточно зруйнувати фінансову систему країни.

За способом ці операції часто вчинюються шляхом розкрадання матеріальних, грошових коштів чи вільноконвертованої валюти, що проводиться з використанням чекових книжок у комбінації з кредитовими та дебетовими авізо. Механізм розкрадання за допомогою чекової книжки у комбінації з кредитовим і дебітовим авізо розрахований на розкрадачів, які ставлять собі за мету «відмити» фіктивно утворені кошти і користуватися ними у легальному платіжному обігу. За технологією виконання суб'єктом цього злочину є посадові особи неплатоспроможних чи платоспроможних підприємств і обслуговуючих їх банків, які діють завжди у змові. З метою більш глибокого маскування процесу «відмивання» фіктивно утворених сум до злочину залучаються підприємства-одержувачі коштів за незабезпеченими чеками. Між підприємством-псевдоплатником і псевдоодержувачем складаються фіктивні угоди, за домогою яких провадиться серія перерахувань з метою завуалювати джерело та ініціатора фіктивно утворених коштів.

Один із видів розкрадання матеріальних або грошових коштів провадиться за допомогою незабезпечених чекових книжок. В основі механізму вчинення таких

злочинів є також утворення фіктивних грошових коштів та їх випуск у безготівковий платіжний обіг. Засобом «відмивання» таких коштів є використання незабезпечених чекових книжок при взаєморозрахунках суб'єктів фінансово-господарської діяльності, тобто підприємств, організацій та установ, в тому числі банківських та інших кредитно-фінансових закладів.

Оформлення незабезпечених чекових книжок може провадитися від імені псевдопідприємств, неплатоспроможних та платоспроможних підприємств.

Неплатоспроможні підприємці-шахраї та їх співучасники-банківські працівники на шляху відмивання фіктивно утворених коштів та їх матеріалізації у товар, готівку чи вільноконвертовану валюту іноді вступають у змову почергово з кількома підприємствами (на території України), роблять два-три цикли перекладання фіктивно утворених сум перед тим як їх матеріалізувати у цінності. Мета цих дій одна – завуалювати джерело та ініціаторів фіктивно утворених коштів та ускладнити перевірку і збір доказів про злочинну діяльність зловмисників. В умовах інтернаціоналізації злочинності та процесуальних бар'єрів, які виникли з розпадом єдиного правового поля між країнами колишнього СРСР, це досить ефективно слугує злочинцям.

Аналогічним способом вчинюються злочини, коли фіктивне платіжне доручення, а услід за ним і фіктивне авізо оформляються від імені неплатоспроможної організації. Хоча на рахунку підприємства-платника кошти є, але у змові з банківськими працівниками з його рахунку під суму, вказану у загальних фіктивних платіжних документах, грошові кошти не знімаються. Для розрахунку під ту чи іншу угоду шляхом службового підлогу направляється фіктивно утворена сума. Як і в попередньому випадку, операція не реєструється у документах дня аналітичного і синтетичного обліку. При викритті таких злочинів шахраї, як правило, висувають алібі, що вони мали сумнів відносно своїх партнерів щодо поставки останніми цінностей, обумовлених в угоді, але мали намір розрахуватись реальними коштами після того, як товари постачальником будуть їм відвантажені або доставлені.

Попередження такого зловживання на початковій стадії викликає ускладнення при доказуванні суб'єктивного боку складу злочину, тобто злочинного наміру шахраїв. Тому правильний вибір моменту легалізації матеріалів – перевірки – має важливе значення.

Варті окремої уваги зловживання за допомогою платіжного доручення у супроводі фіктивного кредитового авізо. В основі цього виду зловживань є незабезпечене коштами платіжне доручення підприємства та фіктивне кредитове авізо банку. Відповідна кваліфікація дій правопорушників залежить від суб'єкта чи варіанта використання цих платіжних документів.

До цієї групи способів провадження незаконних операцій у КБС відноситься також розкрадання коштів чи ВКВ з використанням чекових книжок у комбінації з кредитовим та дебітовим авізо; створення фіктивних підприємств.

Різке зростання злочинності в економічній сфері викликає справедливе занепокоєння, а також необхідність прийняття заходів, і перш за все правового регулювання кредитно-фінансової сфери та підвищення відповідальності за правопорушення в цій сфері.

Відмиванням грошей називається процес, шляхом якого приховується справжнє походження та, в деяких випадках, справжній власник грошей чи іншого

майна. При складній організації системи відмивання грошей, вона включає також і прикриття для джерела їх походження. Для багатьох різновидів діяльності, як відверто кримінальної, так і просто суспільно не прийнятої, відмивання грошей є життєво необхідним процесом. Відмиваються гроші, отримані від наркобізнесу, інших форм організованої злочинної діяльності, з метою ухилення від сплати податків, прикриття корупції офіційних осіб. Зростаюча інтегрованість світової фінансової системи, ліквідація бар'єрів для переміщення капіталу, сприяє спрощенню процесу відмивання і, відповідно, ускладнює процес його моніторингу.

Процес відмивання грошей з певною мірою умовності поділяється на три фази: розміщення, розшарування та інтеграція.

Розміщення – це стадія, на якій гроші, переважно у формі готівки, вводяться до фінансової системи. Ця фаза є найнебезпечнішою з точки зору можливості виявлення правоохоронними та іншими контролюючими органами. Готівкові гроші розміщуються у банках, обмінних пунктах, страхових компаніях, брокерських конторах, шляхом поштових переказів і т. ін. або у закладах, що інтенсивно працюють з готівкою, – ресторанах, казино, магазинах, у першу чергу таких, що торгують коштовними речами. Використовуються імпортно-експортні компанії, фірми з торгівлі нерухомістю. Казино переводять гроші у фішки, потім у зворотному порядку – фішки у готівку чи чеки. Саме на цій фазі найефективнішою є протидія відмиванню грошей, причому на перше місце тут виходять не правоохоронні заходи, а застосування ефективних регуляційних правил для фінансової системи.

Розшарування (або ешелонування) – це стадія, на якій гроші відмежовуються від джерела свого походження шляхом створення складних «шарів» фінансових трансакцій, зокрема, із застосуванням банківських рахунків на підставних осіб. Метою є ускладнення моніторингу їх переміщення та надання анонімності. Цей процес також включає зміщування «законних» та «незаконних» прибутків, використання накладних та акредитивів на неіснуючі поставки, перекази на підставні фірми.

Інтеграція – це фаза, на якій грошам надається видимість отриманих законним шляхом. Незаконні надходження повертаються в економіку шляхом банківських позик, що не викликає потреби у сплаті податків, через придбання коштовних речей, таких, як нерухомість, акції та облігації.

Відмивання грошей у країнах колишнього Радянського Союзу інколи плутають з досить відмінним процесом, що має іншу мету, але деякі спільні риси у реалізації, – мається на увазі виток капіталу. Насправді це зовсім різні процеси, які мають різні цілі, але механізми їх проведення однакові в тому, що обидва передбачають використання складних схем переміщення грошових коштів. В той же час, і більш-менш «класичне» відмивання грошей має місце – значні обсяги грошей, що приховуються від податків, потребують легалізації, так само, як і гроші, отримані за фальшивим авізо, незаконними банківськими кредитами, іншим злочинним шляхом, якщо їх передбачається залучити до легальної економіки. Процес витоку капіталу сам по собі також передбачає його легалізацію, якщо гроші планується інвестувати в економіку країн, що мають строгі регуляційні правила та відповідне законодавство. Схеми з приховання джерела грошей використовуються і в тому разі, якщо потрібно приховати не стільки джерело коштів, скільки їх власника.

Одним із методів розміщення грошей у фінансових інститутах є «смарфінг». При використанні «смарфінга» значні суми грошей розбиваються на менші за встановлений поріг і розміщуються у фінансових установах. Для цього використовується значна кількість осіб («смарфів»), що й проводять таке розміщення.

Інший спосіб розміщення передбачає використання «інсайдерів» – осіб, що використовують тим чи іншим шляхом своє корпоративне становище для власного збагачення. Проблема «інсайдерів» виходить за межі відмивання грошей і стосується широкого кола зловживань корпоративним службовим становищем та зловживань довірою.

Ще один спосіб, що використовується при розміщенні готівки – через «альтернативну» банківську систему. Системи такого роду існують протягом століть, замінюючи собою традиційні банківські, мають відділення в країнах Заходу, де переважно і отримуються гроші, що їх потрібно відмити.

Окрім наведених засобів, можуть використовуватися і перекупка коштовних речей, експортно-імпортні операції, фірми-прикриття тощо. Змішування має місце тоді, коли злочинна організація комбінує незаконно здобуті гроші із законними, а потім репрезентує всю суму як прибуток від законного бізнесу.

Фірми прикриття – законно зареєстровані компанії, що займаються законним бізнесом, але в той же час виступають як прикриття для незаконних операцій, в цьому випадку – для відмивання коштів.

При розшаруванні грошей використовується незаконна банківська система. В цьому разі кримінальне угруповання набуває права власності над банком, потім засновує фіктивну фірму. Банк надає фірмі кредит, отримані гроші перераховуються на банківський рахунок, що належить угрупованню. Фіктивна фірма заявляє про неможливість повернення кредиту, отримує додатковий кредит для сплати відсотка за вже отриманим кредитом.

Відмивання грошей передбачає також витрати для приховання грошей від правоохоронців та інших компетентних органів. І доти, доки гроші знаходяться у процесі відмивання, вони не можуть бути використані. Таким чином, злочинець зацікавлений у скороченні часу, що витрачається на відмивання. Серед «відмивачів» поширюється тенденція повернення до старої практики – контрабанди готівки. Контейнерні перевезення є найбільш зручним для цього засобом, оскільки дозволяють направити готівку у значній кількості до будь-якої країни без відповідних записів.

Трансакції, спрямовані на приховування джерел коштів, структуруються таким чином, що отримання доказів для суду стає практично неможливим. Хоча в деяких випадках вдається в ході розслідування підняти кілька шарів, через які проводилися гроші, і навіть виявити першоджерело. Трансакції слідують не одна за іншою, а паралельно, угоди об'єднуються та роз'єднуються. Найбільш вразливим є момент, коли гроші потрапляють до банківської системи, – саме тоді регуляційні правила, що вимагають проведення фінансовим сектором відповідної перевірки, є найефективнішими.

В останні роки багато уваги надається використанню новітніх технологій при відмиванні коштів. Кримінальні структури у повній мірі користуються перевагами технічного прогресу, зокрема, в сфері телекомунікацій, в першу чергу системи електронного зв'язку, мережі «Інтернет», мобільних телефонних комунікацій.

Закони по боротьбі з відмиванням грошей, що впроваджуються в різних країнах, оперують на трьох рівнях. По-перше, вони накладають певні обов'язки на осіб, що мають справу з грошима інших людей, проводити записи і звітувати стосовно трансакцій, що перевищують певну суму. Це законодавство спрямовано на виявлення відмивання грошей, коли останні потрапляють або знаходяться у фінансовій системі. По-друге, закони передбачають кримінальну відповідальність за сприяння процесу відмивання, усвідомлюючи чи маючи підозру, що власність набуто шляхом вчинення злочину. По-третє, низка обов'язків покладається на осіб, що регулярно мають справу з грошима інших осіб. Звичайно, вони повинні знати, хто їх клієнти, належним чином реєструвати трансакції і до певної міри вживати заходів щодо з'ясування природи трансакцій. Ці правові акти підкріплюються іншими законами та регуляційними правилами.

Окрім внутрішніх ініціатив існує низка міжнародних проектів, спрямованих на вдосконалення взаємодії та сприяння проведенню спільних розслідувань. В національних законах з цього питання зазначається можливість проведення розслідування за інформацією від інших країн.

Закони і процедури, що покладаються на потребу у встановлення зв'язку між злочином та майном, приречені бути недієвими. У кримінальному судочинстві немає і ніколи не буде ресурсів, які могли б бути виділені на встановлення зв'язків за стандартом, необхідним для судового розгляду кримінальної справи. Законодавство з відмивання коштів повинно використовувати механізми, що застосовуються у антикорупційному законодавстві окремих країн, за яким відповідальність за пояснення походження коштів, у певних ситуаціях, покладається на власника.

Міжнародна законодавча база з питань боротьби з відмиванням грошей повинна базуватися на таких основних принципах: криміналізація відмивання коштів дозволяє інкримінування відмивання як злочинної діяльності; вдосконалення законодавства з питань припинення права власності, причому доцільним є впровадження саме цивільно-правової відповідальності за володіння коштами, отриманими від незаконної діяльності; реалізація системи з інформування відповідного регуляційного органу щодо трансакцій, що викликають підозру; це вимагає впровадження системи активного співробітництва між фінансовим сектором і державним регуляційним органом; впровадження системи контролю за грошовими переказами за кордон і з-за кордону; обмеження банківської таємниці, доступ до банківських рахунків з відповідної санкції суду, ліквідація анонімних та «номерних» рахунків.

Цивільно-правова сторона такого законодавства повинна передбачувати: визнання угод, які укладаються щодо фінансових засобів, майна чи майнових прав, що є доходом від злочинної діяльності, недійсними, із настанням наслідків недійсних угод, які провадяться з метою, що суперечить інтересам суспільства та держави; покладання на громадян, котрі укладають майнові договори, провадять операції з фінансовими засобами, майном та майновими правами на суму, що перебільшує окремий, встановлений законом, мінімум, та/або за певних обставин, що вказують на можливий протиправний характер набуття майна, відповідальності за підтвердження законності їх походження.

Існуючий перелік НБУ ознак сумнівних операцій не є вичерпним. В кожній конкретній ситуації банки повинні виходити з того, чи відповідає характер

здійснюваної операції її кінцевим наслідкам, а також чи існує зв'язок між здійснюваною операцією та характером діяльності, фінансовим станом клієнта, а також враховувати регулярність провадження ним операцій за рахунком.

Одна з вирішальних умов економічної безпеки, успіху в євроінтеграції – постійне вдосконалення законодавства, спрямованого на протидію легалізації «брудних» коштів.

Боротьба з легалізацією доходів, здобутих незаконним шляхом, – це один із чинників економічної безпеки України. Нині щонайсерйозніше занепокоєння викликають саме втрати, яких завдає відмивання грошей господарському комплексові. Воно тісно пов'язане з такими явищами, як відплив капіталу, використання для його приховування офшорів. Це одна з головних причин несприятливого інвестиційного клімату в Україні. Боротьба з легалізацією «брудних» коштів необхідна, зокрема, щоб захистити вітчизняну фінансову систему від негативного впливу світового кримінального капіталу.

Але самими кримінально-правовими засобами досконалу систему протидії відмиванню не створити. Сюди треба долучати ще й заходи у сферах адміністративного, фінансового законодавства. Лише така цілісність може стати правовим підґрунтям для виваженої та послідовної державної політики у цій галузі.

Створення ефективної системи заходів із запобігання і боротьби з легалізацією брудних коштів є завданням загальнодержавного рівня, реалізація якого дасть можливість своєчасно виявляти та припиняти злочинний бізнес, що продукує сумнівні доходи.

Важливу роль у захисті БСУ в сучасних умовах відіграють заходи із захисту електронних і пластикових платіжних засобів. В БСУ набуває широкого використання такий вид платіжних засобів, як електронні або пластикові платіжні гроші, а також запроваджена комп'ютеризація міжбанківських розрахунків. Ця обставина сприяла виникненню змін у техніці вчинення низки злочинів у сфері банківської діяльності. Причому тенденція така, щоб чим активніше запроваджуються досягнення техніки та електронні розрахунки у наданні фінансових послуг, тим більш досконалою стає технологія вчинення злочинів з використанням електронних систем, а кількість таких злочинів постійно прогресує.

Під безпекою АСОІБ слід розуміти їх властивість, що виражається в здатності протидіяти спробам нанесення збитку власникам і користувачам системи при різних (навмисних і ненавмисних) діях. Тобто захищеність від випадкового чи навмисного втручання в процес функціонування цієї системи, а також від спроб розкрадання чи руйнування її компонентів. Безпека АСОІБ досягається забезпеченням конфіденційності оброблюваної нею інформації, а також цілісності й доступності компонентів і ресурсів системи.

Розрізняють зовнішню і внутрішню безпеку АСОІБ.

Кожну систему обробки інформації захисту варто розробляти індивідуально з огляду на такі особливості: організаційну структуру банку; обіг і характер інформаційних потоків (усередині банку в цілому, усередині відділів, між відділами, зовнішніх); кількість і характер клієнтів; графік добового навантаження.

Основні етапи побудови системи захисту такі: аналіз, розробка системи захисту (планування); реалізація системи захисту; супровід системи захисту.

За способами здійснення всі заходи забезпечення безпеки комп'ютерних систем поділяються на: правові, морально-етичні, адміністративні, фізичні і технічні (апаратні й програмні).

До правових заходів захисту відносяться чинні закони, укази, постанови й інші нормативні акти, що регламентують правила роботи з інформацією обмеженого використання і відповідальність за їх порушення. Вони перешкоджають несанкціонованому використанню інформації та є стимулюючим чинником для потенційних порушників.

До морально-етичних заходів протидії відносяться всілякі норми поведінки, що традиційно складаються в міру поширення ЕОМ у БСУ. Ці норми здебільшого не є обов'язковими як законодавчо затверджені, однак їхнє недотримання призводить зазвичай, до падіння авторитету, престижу людини чи групи осіб. Морально-етичні норми бувають як неписані (наприклад, загальновизнані норми честі, патріотизму і т.ін.), так і оформлені в кодекс чи правила. Найхарактернішим прикладом останніх є «Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США». Зокрема, вважаються неетичними навмисні чи ненавмисні дії, що викликають додаткові невиправдані витрати ресурсів (машинного часу, пам'яті, каналів зв'язку тощо); порушують цілісність збереженої й оброблюваної інформації; зачіпають інтереси інших законних користувачів і т. ін.

Адміністративні заходи захисту – це заходи організаційного характеру, що регламентують процеси функціонування системи обробки інформації, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб якнайбільше ускладнити чи унеможливити реалізацію загроз безпеці. Вони включають: розробку правил обробки інформації в АСОІБ; заходи, вжиті при проектуванні, будівництві й устаткуванні обчислювальних центрів та інших об'єктів АСОІБ (урахування впливу стихії, пожеж, охорона приміщень, організація захисту від установки апаратури, що прослухує, тощо); заходи, вживані при підборі й підготовці персоналу (перевірка нових співробітників; ознайомлення їх з порядком роботи з конфіденційною інформацією, з мірами відповідальності за порушення правил її обробки; створення умов, за яких персоналу було б невигідно припускатися зловживань і тощо); організацію обліку, збереження, використання та знищення документів і носіїв з конфіденційною інформацією.

Фізичні засоби захисту – це різного роду механічні, електро- чи електронні пристрої та обладнання, спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів системи й інформації, що захищається, організація надійного пропускного режиму.

Технічними засобами захисту є різні електронні пристрої та спеціальні програми, що виконують (самостійно чи в комплексі з іншими засобами) функції захисту (ідентифікацію й аутентифікацію користувачів, розмежування доступу до ресурсів, реєстрацію подій, криптографічний захист інформації тощо).

Найкращі наслідки досягаються за системного підходу до питань забезпечення безпеки АСОІБ і комплексному використання різних засобів захисту на всіх етапах життєвого циклу системи, починаючи із самих ранніх стадій її проектування.

У цій сфері важливо відпрацювати управління засобами захисту і відновлення та політику безпеки.

Політика безпеки – це набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях.

Основними функціями, які мають виконувати ядро безпеки разом з іншими службами, є :ідентифікація, аутентифікація та авторизація; контроль входу користувача в систему і управління паролями; реєстрація і протоколювання, аудит; протидія «збору сміття»; контроль цілісності суб'єктів; контроль доступу.

У чистому вигляді розглянуті принципи реалізації політики безпеки застосовуються рідко. Зазвичай використовуються різні комбінації. Політика безпеки і механізми підтримки її реалізації утворюють єдине захищене середовище обробки інформації.

Існують два підходи до забезпечення безпеки АСОІБ – фрагментарний і комплексний.

Управління інформаційними потоками застосовується, звичайно, в межах вибіркової чи повноважної політики, доповнюючи їх і підвищуючи надійність системи захисту.

Система безпеки центральної АСОІБ повинна включати багаторівневий контроль доступу до периферійних пристроїв і центральної бази даних.

Сфера інформаційної безпеки – найбільш динамічна галузь розвитку індустрії безпеки в цілому. Якщо забезпечення фізичної безпеки має давню традицію й устояні підходи, то інформаційна безпека постійно вимагає нових рішень, тому що комп'ютерні та телекомунікаційні технології постійно обновляються, на комп'ютерні системи покладається усе більша відповідальність.

Безпека електронних банківських систем залежить від великої кількості факторів, які слід враховувати ще на етапі проектування цієї системи.

Автоматизація і комп'ютеризація банківської діяльності (і грошового обігу в цілому) продовжує зростати. Основні зміни в банківській індустрії за останні десятиліття пов'язані саме з розвитком інформаційних технологій. Можна прогнозувати подальше зменшення обороту готівки і поступовий перехід на безготівкові розрахунки з використанням пластикових карток, мережі Інтернет і терміналів управління рахунком юридичних осіб, зростання кількості злочинів з використанням електронних і пластикових платіжних засобів.

У зв'язку з цим варто очікувати на подальший динамічний розвиток засобів інформаційної безпеки банків, оскільки їхнє значення постійно зростає.

Багато в чому прибутковість банку залежить від забезпечення вищого керівництва потрібною, своєчасною і точною інформацією. Системи управління інформацією повинні бути справжніми помічниками в діяльності банку, забезпечуючи, наприклад, інформацією про положення на ринку, прибутковість банківської продукції, становище клієнтів тощо. Отримана з їх допомогою інформація може використовуватися банком для поліпшення обслуговування клієнтів чи для представлення їм з метою використання у власних інтересах.

Банкам потрібна постійна інформація про ступінь ризику їхньої діяльності. Оцінка ризику – це процес, що докорінно може бути змінений за допомогою

сучасних технологій. Сучасні технології дають банкам величезні переваги в організації систем доставки товарів і послуг. Використання електронних засобів зв'язку дозволяє реалізувати: електронні платежі і розрахунки в точці продажу; клієнтські термінали, що тримають прямий зв'язок з банком; домашнє банківське обслуговування за допомогою персонального комп'ютера чи телефону; обмін електронними даними в мережі з розширеним набором послуг; технології електронних банківських карт, включаючи магнітні пластикові й інтелектуальні карти.

Протидія комп'ютерній злочинності передбачає перш за все створення відповідної законодавчої бази, комплексу організаційних заходів, у тому числі підготовку кадрів високої кваліфікації, а також відповідне спеціальне технічне забезпечення.

Реалії сьогодення вимагають активного формування відповідних підрозділів у МВС, СБУ, ДПА України.

В Україні кримінальна відповідальність за посягання у сфері комп'ютерної інформації (її ще називають «комп'ютерна» або «кіберзлочинність») була встановлена лише у 1994 р.

В той же час Україна відстає у створенні відповідної нормативної бази. У новому КК України існує три статті, що передбачають відповідальність за злочини аналізованого виду. Вони об'єднані розділом XVI Особливої частини, який має назву «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». КК України містить й інші статті, які можуть застосовуватись при визначенні відповідальності за вказані посягання. Зокрема, ч.3 ст.190 (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки) і ст.200 (використання підроблених електронних засобів доступу до банківських рахунків).

В Україні немає серйозних наукових розробок проблем небезпечних діянь у сфері комп'ютерної інформації та кримінологічних проблем запобігання цим злочинам. У небагатьох публікаціях на вказану тему неконкретно розглядається коло питань, пов'язаних зі злочинами зазначеного виду.

Єдиний правильний підхід до створення загального поняття злочинів у вказаній сфері полягає у одночасному врахуванні (як їхніх ознак) предмета і знарядь вчинення цих посягань. Спираючись тільки на таке поєднання ознак складу злочину, можна створити «формулу», яка дозволила б безпомилково відрізняти злочини у названій сфері від інших суспільно небезпечних діянь.

Особливість аналізованих посягань у тому, що вони вчиняються у віртуальному просторі. У ньому набуває вияву суспільно небезпечне діяння, починають проявлятися суспільно небезпечні наслідки і навіть знаряддя вчинення злочину є віртуальними... Сутність механізму вчинення злочинів у сфері комп'ютерної інформації полягає у тому, що винний використовує одну комп'ютерну інформацію (знаряддя) для здійснення злочинного впливу на іншу комп'ютерну інформацію (предмет). Саме такий механізм надає цим посяганням виключної специфічності, яка, зокрема, зумовлює потребою у створенні спеціальних кримінально-правових норм про відповідальність за злочини у сфері комп'ютерної інформації. Зазначена інформація є лише предметом або тільки знаряддям вчинення злочину, останній має кваліфікуватися залежно від направленості умислу винного та фактичних наслідків вчиненого.

Родовим об'єктом аналізованих посягань потрібно визнати суспільні відносини у сфері комп'ютерної інформації.

Потрібно також згадати форму вини, з якою вчиняються злочини у сфері комп'ютерної інформації. Для останніх характерна лише умисна форма, яка є однією з основних ознак злочинів у цій області, що має враховуватися при створенні теоретичного визначення таких суспільно небезпечних діянь. Необережне вчинення посягання, яке певним чином пов'язане з комп'ютерними системами і телекомунікаційними мережами, повинне кваліфікуватися за іншими, загальними, нормами КК України.

Комп'ютерні злочини умовно поділяються на чотири основних види: шахрайство і маніпуляції з інформаційною технікою; незаконне використання машинного часу; розкрадання програм (економічний шпіонаж) та комп'ютерний саботаж.

До шахрайства і маніпуляції з інформаційною технікою відноситься неправомірна заміна носіїв інформації та програмного забезпечення, а також несанкційований доступ до процесу обробки відомостей.

Незаконне використання машинного часу полягає у неправомірному використанні у своїх особистих цілях ЕОМ.

До комп'ютерного саботажу відноситься: стирання, приведення у непридатний стан або фальсифікація інформації, пошкодження засобів інформаційної техніки, нав'язування захисту комп'ютерних систем і комп'ютерне вимагання (різновидність рекета), використовуючи недосконалість технічного захисту комп'ютерних систем.

Практика кримінального переслідування за такі злочини в Україні дуже незначна і її можна охарактеризувати тільки у загальних рисах. Тут дії, пов'язані із злочинним посяганням на власність банків та їх клієнтів через комп'ютерні технології можуть кваліфікуватися тільки за ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення»; ст. 222 «Шахрайство з фінансовими ресурсами» або ст. 194 «Умисне знищення або пошкодження майна» (якщо вважати пластикову картку майном) КК України.

Використання в злочинних цілях пластикових платіжних засобів передбачає виготовлення певних документів: пластикової картки, сліпів із неї, звітів матеріально відповідальних осіб, документів-посвідчень особи-пред'явника пластикових карток.

Найбільшу загрозу для системи платежів представлять злочини з підробленими пластиковими картками з використанням справжніх номерів справжніх карток.

При підробці кредитних карток в основному використовуються номери діючих карток з великим невитраченим лімітом – «золоті» або «бізнес»-картки. Вони мають досить велику мережу за сумою і часом використання, їх рахунки не так суворо перевіряються. Це дозволяє збільшити період часу для вчинення шахрайських дій і подовжує термін «життя» карток.

Пластикові картки, викрадені у їх держателів в одній країні, можуть бути використані в іншій. Злочинці пред'являють для оплати товарів і послуг ці пластикові картки, видаючи себе за їхніх законних держателів.

Халатне ставлення окремих службовців банку до збереження службової інформації або недбале збереження пластикових платіжних засобів, умисне

співробітництво банківських службовців із злочинцями сприяє злочинним посяганням з використанням пластикових карток, а також те, що бланки, які використовують для оформлення сліпів, не в усіх банках є бланками суворої звітності, що полегшує доступ до них шахраям.

Для запобігання, виявлення, розкриття і розслідування злочинів, пов'язаних з використанням пластикових платіжних засобів, потрібна взаємодія між правоохоронними органами і службами безпеки платіжних систем.

Надійним механізмом попередження й профілактики злочинних посягань з використанням пластикових платіжних засобів є побудова і реалізація комплексної, багатофункціональної системи безпеки пластикових платіжних засобів.

Система захисту електронних банківських документів охоплює всі етапи розробки, впровадження й експлуатації програмно-технічного забезпечення інформаційно-обчислювальної мережі та включає чіткий розподіл відповідальності на кожному етапі підготовки, обробки і виконання електронних банківських документів на всіх рівнях. Вона є єдиною для усіх інформаційних завдань НБУ і СЕП. Для підвищення ступеня захисту електронних розрахункових документів у СЕП повинні використовуватися додаткові засоби, включаючи бухгалтерський контроль. Технологічні та криптографічні засоби безпеки слід використовувати не тільки в СЕП, а й у всіх інформаційних системах НБУ, що підвищить гарантії захисту банківської таємниці.

Банківська таємниця – це відомості, що не підлягають розголошенню і охороняються державою як службова таємниця. До них належить визначений Законом перелік відомостей про стан рахунків клієнтів, виконуваних операцій тощо. Банківська таємниця є різновидом комерційної таємниці, яка забезпечує банку одержання найвищих прибутків.

Співвідношення державної та банківської таємниці полягає в такому. Банківська таємниця не відноситься до відомостей, які становлять державну таємницю, а режим її охорони визначається банками. На відміну від банківської таємниці, режим секретності державної таємниці встановлюється виключно законами і підзаконними актами України, а Звід відомостей, що становлять державну таємницю, затверджується наказом Голови СБ України.

Згідно із чинним законодавством, розголошення державної, як і комерційної таємниці, тягне за собою також кримінальну відповідальність, а банківської – лише адміністративну (цивільну, дисциплінарну – в першому і другому випадках).

Комерційною таємницею є лише така інформація, яка відповідає певним вимогам: комерційна цінність інформації; секретність інформації; вжиття заходів, направлених на збереження секретності такої інформації.

Після визначення і затвердження наказом керівника підприємства переліку відомостей, що становлять комерційну таємницю, визначаються конкретні заходи, які підприємство буде вживати для їх охорони. Серед них є розробка і затвердження: правил внутрішнього трудового розпорядку; положення про охорону комерційної таємниці; інструкції про документообіг та роботу з документами; посадових інструкцій про дотримання співробітниками режиму нерозголошення комерційної таємниці; включення до тексту статуту підприємства розділів, які регламентують порядок охорони комерційної таємниці; типової угоди про нерозголошення комерційної таємниці, яка укладається з особами, котрі мають доступ до такої

інформації; додаткової угоди до трудового договору чи контракту про нерозголошення найманими працівниками комерційної таємниці.

Надання відповідним відомостям статусу банківської або комерційної таємниці є одним із способів запобігання несанкціонованому використанню цінної інформації.

Для комерційної таємниці важливим є охорона суті та змісту інформації, для банківської – не тільки суті відносин між банком і клієнтом, а й, як правило, самого факту наявності таких відносин. Комерційна таємниця може бути надана власником третій особі за плату. Надання банківської таємниці третій стороні є порушенням закону. Охорона комерційної таємниці – турбота її власника, а банківської – банку. Охорона банківської таємниці визначається не міркуванням прибутковості, а нормою закону.

Передбачена відповідальність за два склади злочинів: 1) незаконне збирання з метою використання відомостей, що становлять комерційну таємницю; 2) незаконне використання відомостей, що становлять комерційну таємницю, якщо це матеріально зашкодило суб'єкту підприємницької діяльності.

Під незаконним збиранням відомостей, що становлять комерційну таємницю, слід розуміти активні дії, направлені на добування (одержання) таких відомостей будь-яким способом: вилучення, в тому числі викрадення документів, що містять комерційну таємницю, чи предметів, відомості про які становлять комерційну таємницю, незаконне ознайомлення з такими документами чи предметами будь-яким способом, прослуховування телефонних розмов, опитування співробітників суб'єкта підприємницької діяльності, підслуховування усних розмов, одержання таких відомостей від осіб, які ними володіють, за плату чи шляхом застосування погроз, насильства тощо.

Під незаконним використанням відомостей, що становлять комерційну таємницю, слід розуміти впровадження «технічних» таємниць у власне виробництво, врахування здобутих відомостей при плануванні власної підприємницької діяльності, продаж відомостей, що становлять комерційну таємницю, їх розголошення тощо.

Цивільна відповідальність ґрунтується на цивільно-правових відносинах, за яких одна сторона зобов'язана відшкодовувати іншій збитки, завдані протиправними (і не завжди кримінально караними) діями у зв'язку з посяганням на комерційну (банківську) таємницю.

Адміністративна відповідальність за посягання на таємниці банку ґрунтується на положеннях Кодексу України про адміністративні правопорушення. Посягання на таємниці банку законодавством України віднесено до дій, які кваліфікуються як недобросовісна конкуренція.

Дисциплінарна відповідальність за посягання на таємниці банку ґрунтується на засадах трудового законодавства України та нормативної бази самих банків. В останньому випадку відповідальність можуть нести тільки працівники банку.

Систему захисту банківської таємниці в Україні становлять: загальні норми права щодо захисту секретної інформації, які встановлює держава (закони, декрети, укази, постанови); правові норми із захисту секретів, які встановлює керівництво банків (накази, розпорядження, інструкції, пам'ятки тощо); спеціальні структурні

підрозділи банків, які на практиці забезпечують виконання норм прийнятих, державою та адміністрацією. Всі ці елементи тісно пов'язані між собою.

Розголошення комерційної таємниці – це незаконне ознайомлення інших осіб з відомостями конфіденційного характеру, віднесеними суб'єктом підприємницької діяльності до відомостей, що становлять його комерційну таємницю, а так само умисне створення умов, які сприяли ознайомленню з ними сторонніх осіб, вчинене особою, котрій такі відомості стали відомі у зв'язку з професійною чи службовою діяльністю, яка повинна зберігати такі відомості в таємниці.

Всі розглянуті раніше проблеми стосуються людей і залежать від них, що зумовлює потребу підвищення ефективності та практики банківського менеджменту і роботи з персоналом банків.

В основі кадрового менеджменту лежить кадрова політика банку. Сучасна кадрова політика є багатосуб'єктною і визначається насамперед як генеральна лінія, котра забезпечує виявлення наукових принципів підбору, розстановки і використання кадрів, визначення зумовлених конкретними історичними умовами вимог до них, а також завдань, напрямів, форм і методів кадрової роботи.

Кадрова політика на практиці проводиться за допомогою певної системи, що містить окремі дії та операції, а саме: планування і прогнозування потреб у кадрах, їх підбір, оцінка, розстановка, виховання, підготовка, контроль тощо. Основу цієї системи становлять підбір і розстановка кадрів.

Кадровий менеджмент одержав широке визнання у світі, адже він найбільше відповідає потребам і умовам ринкової економіки, є антиподом командно-адміністративного, авторитарного управління. Основними його ознаками як типу управління персоналом вважаються: у центрі управління повинна бути людина з її потребами, інтересами, мотивами, цінностями; перевага надається економічним методам і засобам управління; професіоналізм управління – одна із головних вимог до менеджера; гнучка організація управління здатна швидко змінюватися відповідно до змін середовища. Таким чином, ця діяльність створює психолого-юридичні відносини між об'єктом і суб'єктом управління, сприяє досягненню поставлених цілей шляхом використання мотивів праці та інтелекту людей.

Застосуванню на практиці наукових засад визначення залежності вимог, що висуваються до фахівця, від характеру його діяльності та службового становища сприяє концепція побудови професійно-кваліфікаційної моделі сучасного керівника, яка складається з двох частин. Перша містить функції співробітника у сфері адміністративно-управлінської і професійно-фінансової діяльності. Друга – кваліфікаційні вимоги до морально-етичних, ділових, особистих якостей, знань і вмінь працівника.

Стан економічної безпеки України, сучасне і майбутнє її державності прямо залежить від формування управлінської банківської еліти. Підбір і розстановка таких кадрів повинні здійснюватись у суворій відповідності до вимог, які до них висовуються, згідно із сучасною кадровою політикою, її засадами, чому підпорядкована практика банківського менеджменту.

Банківський менеджмент – це практика управління банківською системою і банківською справою, а також персоналом банків на основі нормативно-правового регулювання цієї діяльності як на загальнодержавному, так і банківському рівнях,

сучасної кадрової політики відповідно до оновлених принципів, форм і методів управління.

Банківський менеджмент можна трактувати і як управління банківською системою (банківською справою), і як управління персоналом (його кадрами).

Такий підхід до організації банківського менеджменту загалом дозволяє підпорядкувати управління БСУ банківському менеджменту, або управляти банківською системою через персонал.

Науково-методичне забезпечення передбачає розробку для банків методики провадження окремих видів операцій, управління активами і пасивами, формування оптимальних портфелів вкладень, мінімізації ризиків тощо. Адже НБУ не в змозі виконувати повною мірою ці функції.

Кадрове забезпечення діяльності банківської системи покликане своєчасно і якісно провадити підбір, підготовку, розстановку, виховання, ротацію банківських службовців. У кількісному відношенні порушену проблему практично вирішено, але тепер постає питання якості підготовки фахівців, що вимагає створення мережі різноманітних навчальних закладів, узгодження навчального процесу із сучасними запитами банків.

Законодавчо-правове забезпечення банківської діяльності передбачає створення належного правового поля, що є вихідним правилом у забезпеченні стабільного функціонування усіх банків. Сукупність чинних законодавчих актів має регулювати не лише загальні моменти діяльності кредитних установ, як тепер, а й окремі аспекти банківської справи в країні (кредитної, депозитної, інвестиційної) та основ діяльності різних елементів банківської системи (зокрема, спеціалізованих комерційних банків різних видів) тощо.

Без сукупності розглянутих елементів інфраструктури нормальне функціонування банків в умовах ринку неможливе або вкрай ускладнене. Тому створення відповідного забезпечення організації банківської справи за різними напрямами слід вважати одним із потрібних моментів подальшого вдосконалення інституційної структури банківської системи. Слід нормативно інтегрувати до банківської системи зазначену сукупність складових, які формують інфраструктуру, що об'єктивно випливає із потреби у всебічному регулюванні діяльності банківської системи.

Банки повинні розробляти концепцію безпеки банку, яка містить: загальні положення, заходи організації безпеки банку, заходи безпеки банку, забезпечення безпеки банківської діяльності.

На основі цієї Концепції банки розробляють Положення про підрозділ безпеки та інші документи щодо реалізації заходів безпеки; окремі положення Інструкції про порядок комплектування персоналу банку.

Аналіз результатів діяльності банків з питань безпеки показує, що не всі банки створюють повну нормативну базу. Відсутність законодавчої і нормативної бази з цих питань часто не дає можливості банкам не тільки регламентувати таку діяльність власними нормативними актами, а й активно здійснювати її.

Слід поєднувати систему заохочень з питаннями безпеки. Кожен член колективу повинен усвідомити (і перевірити на собі), що будь-яка дія, яка зміцнює безпеку банку, її економічну стабільність, буде гідно винагороджена.

Базовим видом діяльності у профілактичній роботі є виховна робота та турбота про людей. Саме фахівці безпеки мають навчити кожного співробітника банку

основам безпеки комерційної діяльності. У першу чергу, навчання повинні пройти співробітники, що працюють з конфіденційними чи матеріальними цінностями. Служба безпеки повинна відслідковувати будь-які зміни в економічній стабільності банку, у мікрокліматі колективу, у поведінці кожного зі співробітників, тому що вони можуть мати найсерйозніші наслідки.

У процесі підбору персоналу найважливішу роль відіграє кадрова служба банку, яка є першою інстанцією у боротьбі за високий рівень банківської установи. До кожної категорії працівників висуваються певні вимоги, деякі з них затверджені законодавчо, інші встановлює сам банк з метою отримання найвищих професійних результатів праці та безпеки своєї установи.

Основними суб'єктами у процесі підбору персоналу постійно є: на першому етапі – кадрова служба банку; на другому – кадрова служба, служба безпеки, керівник відповідного підрозділу; на третьому – керівник, який приймає рішення про зарахування, кадрова та юридична служби, що оформлюють працівника на роботу.

При цьому основні критерії включають вимоги до якостей та знань майбутнього працівника: стосовно віку, статі, сімейного стану, стажу роботи, освіти, а також специфічні вимоги до окремих категорій працівників, що встановлені законодавчо, передусім, це стосується керівників банків.

Порівняно із загальними нормами трудового права в банківських нормативно-правових актах слід враховувати передбачену можливість за ініціативою контролюючого органу – Національного банку – відсторонити посадову особу банку від посади у разі грубого чи систематичного порушення нею Закону про банки або нормативно-правових актів Нацбанку.

Існують певні вимоги до спеціалістів підрозділів банку, які випливають із функцій цих підрозділів. Банки можуть не обмежуватися вимогами до своїх працівників, які встановлені законодавчо. Для підвищення рівня конкурентоспроможності, банками встановлюються додаткові вимоги до своїх службовців. Такі вимоги викладають в положеннях про відповідні підрозділи, посадових інструкціях тощо.

Вітчизняний банківський менеджмент має враховувати зарубіжний досвід, багатий своєю історією і практикою.

Положення передбачає субординацію, порядок призначення та переміщення керівників і фахівців, відповідальність, виконання функцій у просторі й часі. При цьому служба управління персоналом, так само, як і інші підрозділи, повинна визначати стратегію на перспективу розвитку банку. Першочерговим завданням цієї стратегії є укомплектування штабу банку за рахунок фахівців з високою кваліфікацією. Стратегія і тактика стосовно основної задачі містить у собі такі головні моменти: кадрова політика повинна враховувати особливості конкретного банку, його матеріальні й організаційні можливості і провадитися всіма менеджерами банку, а не тільки служби управління персоналом та працівниками вищого ешелону керівництва.

Кадрова робота в банках має одну дуже важливу особливість – працівник постійно має знаходитися під спостереженням. Важливо знати про зміни в характері, появу зв'язків, що ганьблять тощо.

Постійно розширюється сфера банківських послуг, змінюються організаційні структури в зв'язку з кон'юнктурою ринку, банк інвестує різні галузі господарства,

упроваджується нова техніка, використовується Інтернет. Усе це створює передумови для постійного підвищення кваліфікації працівників. Українські банки у своїй більшості не мають стратегічних планів підготовки і перепідготовки співробітників, відсутня потрібна мотивація й об'єктивна оцінка результатів роботи з персоналом, навчання.

Одним з найважливіших підрозділів, без наявності якого ризикована діяльність банку підвищується, є служба безпеки банку. Служба безпеки покликана забезпечити охорону інтересів своєї установи в самому широкому розумінні цього слова. Це включає як організацію фактичної охорони банку, так і забезпечення економічної безпеки. До функцій служби безпеки відноситься перевірка відомостей, які надходять до банку. Це спричиняє потребу у вимозі від працівників служби наявності можливості для такої перевірки. Крім того, дуже важливою є участь працівників служби безпеки у кредитній діяльності банків, у перевірці документів, які надаються позичальником, його репутації, кредитної історії, наявності та фактичного стану забезпечення, яке ним пропонується, платоспроможності позичальника та/або його поручителя, супроводження кредиту, нагляд за його цільовим використанням тощо.

До особливостей функціонування банківських установ, яке зумовлює специфіку трудових правовідносин між банком та працівником, відноситься також те, що в процесі діяльності останні мають допуск до банківської таємниці. Розголошення таких відомостей може завдати матеріальних та моральних збитків клієнту.

Виходячи із огляду основних геоекономічних подій, що відбулись останнім часом, можна дійти висновку: існуюча нині світова система розподілу праці несприятлива для України. У наших найближчих сусідів на Заході справи в економіці не настільки блискучі, як багато кому здається. У більшості з них від'ємні торговельні баланси, тобто вони купують більше, ніж продають.

Україні давно треба було б перейти від екзогенних (зовнішніх) факторів розвитку до ендогенних (внутрішніх). Зазвичай при цьому слід всіляко підтримувати вигідну для країни зовнішню торгівлю. Але вже ні в кого не викликає сумнівів потреба у розширенні та поглибленні внутрішнього ринку, котрий і має освоїти значну частину наявних у країні ресурсів. Від ресурсовидобувної схеми розвитку, що не веде вперед, ми маємо перейти до інноваційної моделі.

Україні слід створити власну модель розвитку, орієнтуючись на ендогенний потенціал, зокрема науковий. Це позбавить залежності від зовнішніх чинників, сприятиме утвердженню суверенітету, за який так довго боролись і який швидко можна втратити.

ДОДАТКИ

Додаток А

ПОНЯТІЙНО-НАУКОВИЙ АППАРАТ, ВИВЕДЕНИЙ* АБО ВИКОРИСТАНИЙ В МОНОГРАФІЇ

БЕЗПЕКА

***Національна безпека України** є предметом комплексного багатогалузевого наукового дослідження та в синтезованому вигляді визначається як такий стан держави, що характеризує сукупність державно-правових і суспільних гарантій, котрі забезпечують потрібний рівень захищеності корінних інтересів людини й громадянина, суспільства й суверенної держави в цілому від явних і потенційних внутрішніх та зовнішніх загроз, їх своєчасного виявлення, запобігання і нейтралізацію, що забезпечує можливість стабільного всебічного прогресу, сталого розвитку суспільства.

Теорія національної безпеки – це метанаука, яка поєднує в собі прикладні аспекти соціальних, воєнних, гуманітарних, технічних, психологічних, біологічних та інших наук з метою дослідження сутності, змісту, методів, форм і засобів забезпечення безпеки особистості та соціальних спільнот різного рівня.

***Державна безпека** – це стан захищеності основ конституційного ладу, політичного, економічного, оборонного, науково-технічного й інформаційного потенціалу країни від зовнішніх і внутрішніх загроз, що виходять від іноземних спецслужб і організацій, а також злочинних співтовариств, груп і окремих осіб.

*__Економічна безпека__ – це такий стан національної економіки, який забезпечує стабільне функціонування виробництва, кредитно-фінансової і банківської системи, задовольняє матеріальні потреби держави, суспільства й особи, здійснює їх захист від зовнішніх і внутрішніх фінансових загроз.

Цінова безпека – різновид безпеки, який може найбільше вплинути на економіку. Правильне визначення ціни дозволяє вірно оцінити працю і

* Виділені цим знаком терміни виведені авторами монографії.

встановити вірний розподіл благ між населенням країни, проводити справедливий обмін послугами і товарами як всередині країни, так і за її межами, на міжнародному рівні. Цінова безпека тісно пов'язана з фінансово-грошовою безпекою.

Фінансово-грошова безпека – такий різновид безпеки, який впливає на всі сфери економіки держави через гроші як еквівалент вартості всіх товарів, які є силою, спроможною через ціну дестабілізувати положення в країні.

Фінансова безпека – це стан захищеності фінансових інтересів держави та інших суб'єктів господарювання стосовно внутрішніх та зовнішніх економічних загроз. Від її рівня залежить інвестиційний клімат у державі. Зумовлена вона стабільністю грошово-кредитної, бюджетної та валютної систем. Визначається такими показниками, як: розподіл державного бюджету, стійкість банківської системи, національної валюти, стан зовнішньої та внутрішньої заборгованості, дефіцит платіжного балансу.

Інформаційна безпека банку це – формування інформаційних ресурсів банку та організація гарантованого їх захисту. Досягається створенням у банку системи збору та обробки інформації, проведенням відповідних заходів щодо її зберігання та розподілу, визначенням категорій і статусу банківської інформації, порядку і правил доступу до неї, дотриманням усіма працівниками, клієнтами та акціонерами банку норм і правил роботи з банківською інформацією, своєчасним виявленням спроб і можливих каналів витоку інформації та їх попередження.

Методологія дослідження БСУ – це система визначених теоретичних принципів, логічних прийомів, конкретних способів дослідження діяльності по формуванню й удосконаленню банківської системи. Теоретичні принципи – історія, єдність логічного й історичного. Логічні прийоми – дедуктивний та індуктивний умовивід, аналіз і синтез, порівняння, узагальнення. Конкретні способи дослідження – інструменти пізнання, застосовувані для встановлення знання про БСУ.

***Безпека банківської системи України** – це такий стан чинних правових норм і відповідних їм інститутів безпеки, який відображає рівень захищеності державою кредитно-фінансових відносин між суб'єктами банківської діяльності та гарантує стійке функціонування всієї банківської системи України; забезпечує можливість повної реалізації та захист життєво важливих фінансових та економічних інтересів держави, суспільства й особи; виключає або максимально обмежує деструктивні наслідки від зовнішніх та внутрішніх загроз, недосконалості зовнішньоекономічної, внутрішньогосподарської та бізнесової діяльності.

***Забезпечення безпеки БСУ** – це процес створення умов для стабільного фізичного розвитку, економічного суверенітету держави; попередження й

усунення загроз, умов і інших факторів, здатних виявити негативний, дестабілізуючий вплив на процеси розвитку національної банківської системи, усунення протиріч між інтересами держави та окремих соціальних груп, суспільства й індивіда. Забезпечення безпеки БСУ являє собою цілеспрямовану, постійно здійснювану діяльність (нормотворча, аналітична, оперативно-розшукова й інша) усіх суб'єктів безпеки БСУ із захисту її життєво важливих інтересів.

***Банк** – це такий інститут ринкової економіки і суб'єкт грошово-кредитних відносин, який приймає депозити, надає кредити, здійснює розрахунки – валютні, касові, інвестиційні, трастові, консультаційні, факторингові, з цінними паперами, з дорогоцінними металами і операції на основі вимог чинного законодавства та нормативних актів, що регулюють діяльність структур, які входять до банківської системи.

Банківська система – це сукупність різних видів банків і банківських інститутів, з допомогою яких здійснюється мобілізація коштів, надаються клієнтурі кредити та різноманітні послуги щодо прийому вкладів і наданих кредитів. Ця система є внутрішньо організованою, взаємопов'язаною, має загальну мету і завдання, завдяки чому являє собою якісно новий, вищий рівень економічних відносин, що характеризуються взаємодією банківських установ, визначаючи їхню роль в економіці як цілісної системи. БСУ є дворівневою.

Перший рівень репрезентує Національний банк України, що є центральним банком України, власністю держави, підзвітним Верховній Раді України, має право законодавчої ініціативи. Він є юридичною особою та емісійним центром України, проводить єдину грошово-кредитну політику, регулює діяльність банківської системи в цілому, організовує і здійснює міжбанківські розрахунки. Другий рівень банківської системи – це комерційні банки різних форм власності, спеціалізації та сфери діяльності.

Вартість товару – це втілені в продукті товарні відносини, які виникають між людьми, що брали участь у виготовленні продукту відповідно до кількості і якості затраченої праці кожним виробником. Відхилення цін від вартості веде до порушення еквівалентного обміну товарами, а отже, й товарних відносин.

КРЕДИТ

Кредитний механізм – це певна сукупність принципів, організаційних форм, методів і правил, що регулюються чинним законодавством і забезпечують необхідні умови реалізації кредитних відносин. Кредитні

відносини виникають між кредитором і позичальником з приводу одержання останнім позички в грошовій або товарній формі на умовах повернення в певний строк із сплатою відсотка. Існують такі види кредиту як – комерційний, товарний, державний, фінансовий, кредит під цінні папери, найбільш поширеною формою якого є банківський кредит.

Банківський кредит надається банками в грошовій формі підприємствам, населенню і державі. Кредитні відносини між банками і клієнтами виникають не тільки при одержанні останніми позички, але й при розміщенні ними своїх заощаджень у вигляді внесків на поточних і депозитних рахунках. Сфера використання банківського кредиту ширша, ніж комерційного. Комерційний кредит обслуговує тільки обіг товарів, а банківський – і накопичення капіталу. Для цього комерційними банками надаються облікові та акцептні кредити, які пов'язані з обігом векселів. Банківський кредит поділяється за строками і видами.

Облікова ставка (discount rate) – це відсоткова ставка, за якою центральний (емісійний) банк надає позики комерційним банкам для їх підтримки. Спрощено облікову ставку можна розглядати як найнижчу кредитку ставку. Зокрема вона є стартовою на кредитних аукціонах НБУ.

Кредитний договір – це цивільно-правова угода банка-кредитора та клієнта-позичальника, якою оформлюється надання кредиту, визначаються взаємні фінансові зобов'язання і юридична відповідальність сторін. Надання банком своїм клієнтам позичок обмежується розміром ресурсів, які він має.

***Кредитно-банківська сфера** – (грец. – "куля") розглядається як галузь діяльності, межа розповсюдження будь-чого, сфера впливу. Сфера, кредитування, є основним визначальним напрямом діяльності всіх видів банків та банківських інститутів, головною ланкою кредитної системи. Доцільність і правомірність самостійного розгляду поняття "кредитно-банківської сфери" обґрунтовується тим, що, кредитування – головна сфера діяльності банків, які, в свою чергу, є головною ланкою кредитної системи.

Кредитна політика охоплює систему фінансово-кредитних заходів держави, її центрального банку, інших виконавчих структур, спрямованих на досягнення певних економічних цілей.

Основними напрямками кредитної політики сьогодні є політика кредитної рестрикції ("дорогих грошей") і політика кредитної екстансії ("дешевих грошей"). Політика рестрикції проводиться в фазі економічного підйому з тим, щоб зменшити кредитування господарства, відтягнути економічний бум і наступний спад. Політика експансії проводиться в фазі економічного спаду з тим, щоб розширити кредитування і тим самим стимулювати економічне пожвавлення і зростання виробництва.

МЕТОДИ І НОРМАТИВИ

Метод фінансово-правового регулювання – це сукупність засобів впливу на учасників фінансово-правових відносин, які характеризуються юридичними фактами, з якими пов'язуються виникнення фінансових правовідносин, правовим статусом їх суб'єктів та розподілом права і обов'язків між ними, видами санкцій за порушення приписів держави і порядком їх застосування.

Державно-нормативний метод регулювання виражається в тому, що держава розробляє і приймає закони та інші форми нормативних актів, що спрямовані на здійснення всієї системи державного управління суспільством, економікою та іншими сферами.

Локальний метод правового регулювання проявляється переважно у формі договору, при якому сторонам надано певну ініціативу, а регулюються питання, які мають значення лише для конкретного підприємства, установи, організації.

Фінансово-правові норми – це обов'язкові розпорядження державних органів з приводу мобілізації, розподілу і використання централізованих і децентралізованих фондів, визначені на підставі законодавчих актів. Вони мають обов'язковий, імперативний характер і сприяють фінансовому регулюванню діяльності.

Фінансове регулювання – це заснований на певних принципах та правовому регламентуванні процес організації фінансових потоків у суспільстві між органами державного управління і підприємствами. Відомі такі два методи розподільних відносин: сальдовий і нормативний.

Сальдовий метод передбачає виділення підсумкового (сальдового) елемента в розподілі доходів.

Нормативи – це абсолютні та відносні величини, які застосовуються для регулювання фінансових відносин; вони виражають загальні вимоги до затрат і результатів виробництва, обміну та розподілу. Нормативи є розрахунковими величинами затрат, тому їх застосовують як показник співвідношення різних показників або для розрахунку деяких показників.

Норми – це узаконені або визнані обов'язковими для використання як певна міра величини показників або поведінки.

***Нормування** – це методика і техніка фінансової діяльності, наукова обґрунтованість нормативів і методик. Нормативне забезпечення фінансового механізму включає в себе: економічні нормативи і норми; інструкції щодо методики чи послідовності фінансових операцій; облік, звітність, розрахунки, інші чинні нормативно-правові акти, які мають забезпечувати успішне функціонування фінансового механізму.

Ліквідність балансу банку – це здатність банку своєчасно й повністю розплачуватися за своїми зобов'язаннями за першою вимогою вкладників. Показники ліквідності балансу комерційного банку встановлюються у вигляді нормативного співвідношення між активами і зобов'язаннями банку з врахуванням строку їх погашення, а також можливості реалізації активів. Максимальний розмір ризику на одного позичальника визначається у відсотковому відношенні до загальної суми власних коштів банку. У розрахунок ризику включається вся сума вкладів і кредитів даному позичальнику, а також видані за його дорученням гарантії, доручення та інші зобов'язання.

***Незаконна операція** в кредитно-банківській сфері – це комплекс цілеспрямованих та логічно взаємопов'язаних незаконних дій, метою яких є отримання надприбутку або досягнення економічного ефекту.

РИЗИКИ

Банківські ризики –це певна ситуаційна характеристика діяльності банку, яка показує невизначеність результату та можливих небажаних наслідків у разі невдачі. Такими наслідками є неотримання прибутку, виникнення збитків, внаслідок невиплат за отриманими кредитами, і т.ін.

За часом ризики розподіляються на ретроспективні, поточні та перспективні. За ступенем: низькі, помірні, повні.

Політичні ризики – це ризики, які зумовлені змінами політичного становища, що негативно впливає на результати діяльності банку (воєнні дії на території держави, блокування кордонів, заборона на вивіз товару тощо).

Економічні ризики – це такі ризики, які обумовлені негативними змінами в економіці країни або самого банку. Найбільш поширеним видом економічного ризику, в якому сконцентровані окремі ризики, є ризик незбалансованої ліквідності, що являє собою неможливість своєчасно виконувати платіжні зобов'язання.

Виробничі ризики – це ризики, що можуть виникнути на виробництві, і які слід враховувати під час складання прогнозів (пов'язані з ризиками затримки у постачанні або недопостачанням матеріалів, сировини, палива, електроенергії, устаткування; чи постачанням їх нижчої якості; ризиками невиходу на роботу головних фахівців тощо).

Комерційні ризики – це ризики, які треба враховувати під час визначення прогнозів. Вони можуть виникнути у процесі реалізації продукції (їх потрібно відрізняти від норм природних втрат, які застосовують до певного виду товарів і продуктів).

Фінансові ризики є найнебезпечнішими, їх дуже важко спрогнозувати (це – передбачуване підвищення податкових ставок посеред фінансового року чи облікової кредитної ставки; певна фінансова стратегія фірми, якщо вона змінює ціни на цінні папери; зміна Національним банком курсу валют тощо).

Зовнішні ризики – це ті ризики, які не пов'язані з діяльністю банку. На їх рівень впливає велика кількість факторів – політичні, економічні, демографічні, соціальні, географічні та ін.

Внутрішні ризики – це ті ризики, які зумовлені діяльністю самого банку, його клієнтів чи конкретних контрагентів. На їх рівень впливає ділова активність керівництва банка, вибір політики та тактики тощо.

Депозитні операції – це операції із залучення коштів юридичних і/ або фізичних осіб у вклади або до запитання, або на визначений термін. Депозити можуть бути терміновими, до запитання, у вигляді заощаджених вкладів фізичних осіб, цінних паперів.

Лізинг – це метод фінансування розвитку нової техніки і технології, розширення продажу обладнання, що особливо актуально за потреби у прискореному впровадженню окремих елементів реального основного капіталу, скороченні життєвого циклу товару і т.ін.

Кліринг – це взаємна оплата між двома банками, районами, економічними одиницями, державами, під час якої проводиться обмін товарами без переведення грошей (валюти).

Кримінальна безпека являє собою такий різновид безпеки, який не має конкретного носія, але дуже впливає на економічне положення держави (економічні злочини, криміналізація суспільства тощо) та її мешканців (вбивства, грабежі, насильство, крадіжки тощо).

Відмивання грошей – процес, шляхом якого приховується справжнє походження та/або справжній власник грошей чи іншого майна. Відмиваються гроші, отриманні від наркобізнесу, інших форм організованої злочинної діяльності, з метою ухилення від сплати податків, прикриття корупції офіційних осіб.

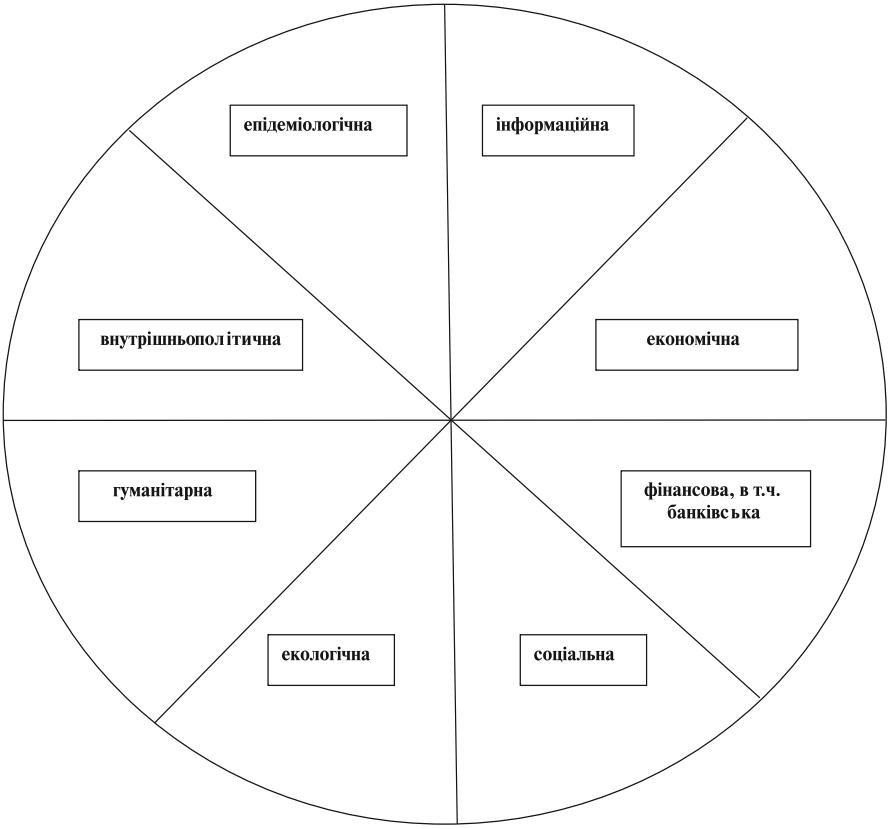
***Банківська таємниця** – це відомості, що не підлягають розголошенню і охороняються державою, як службова таємниця. До них належить визначений законом перелік відомостей про стан рахунків клієнтів, виконуваних операцій тощо. Банківська таємниця хоча і не відноситься до державної таємниці, є різновидом комерційної таємниці, яка забезпечує одержання найвищих прибутків.

***Сучасна кадрова політика** є багатосуб'єктною і визначається насамперед як генеральна лінія, котра забезпечує виявлення наукових принципів підбору, розстановки і використання кадрів управління, визначення зумовлених конкретними історичними умовами, вимог до них, а також завдань, напрямків, форм і методів кадрової роботи.

***Банківський менеджмент** – це практика управління банківською системою і банківською справою, а також персоналом банків на основі нормативно-правового регулювання цієї діяльності як на загальнодержавному, так і банківському рівнях сучасної кадрової політики відповідно до принципів, форм і методів управління.

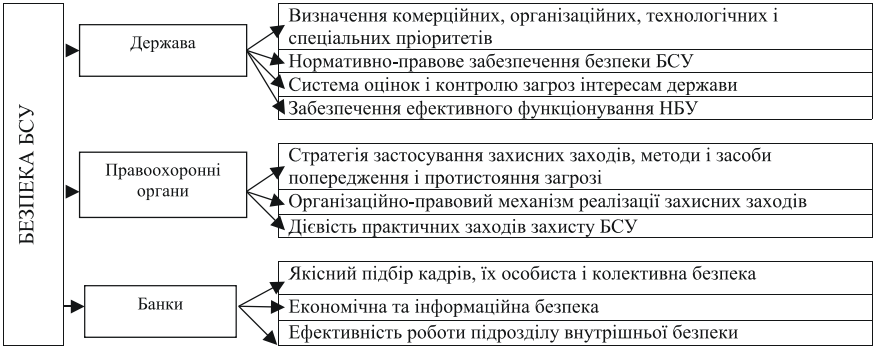
Додаток Б.1.

Складові внутрішньої безпеки України



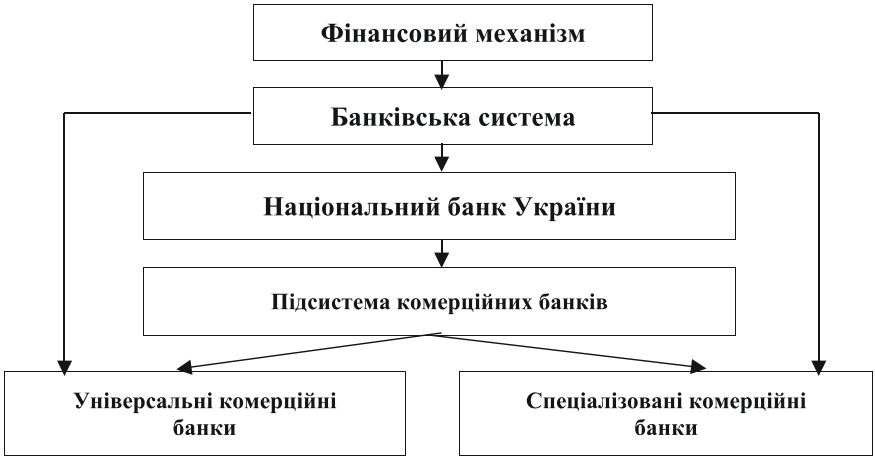
Додаток Б.2.

Система забезпечення безпеки банківської системи України



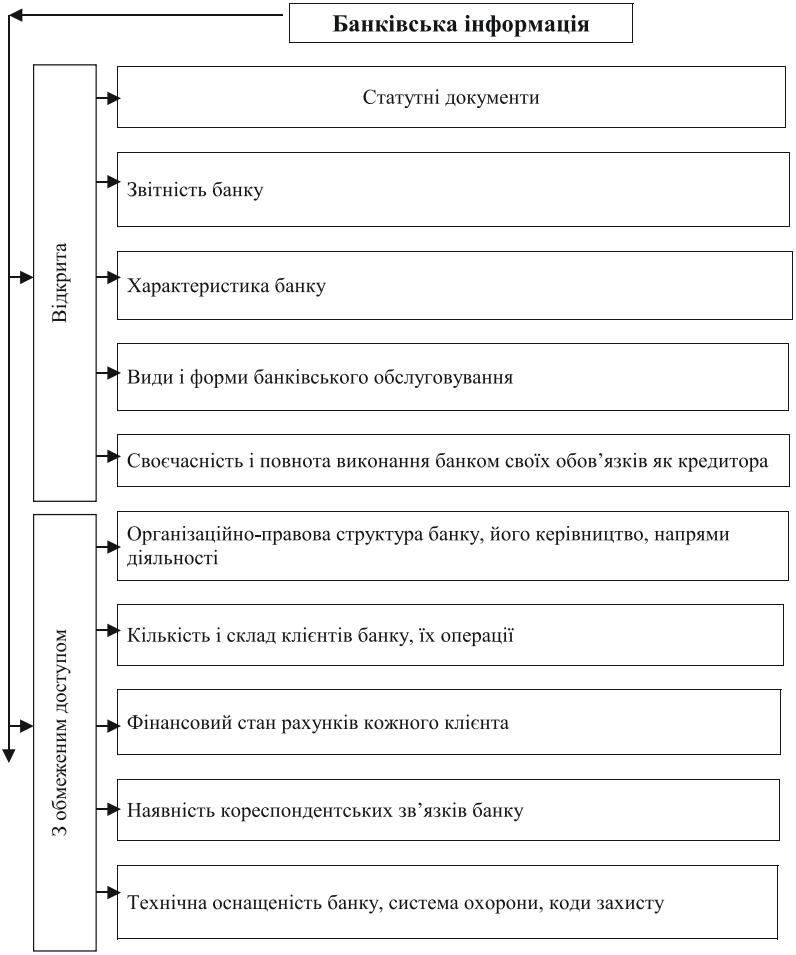
Додаток Б.3.

Структура побудови банківської системи України



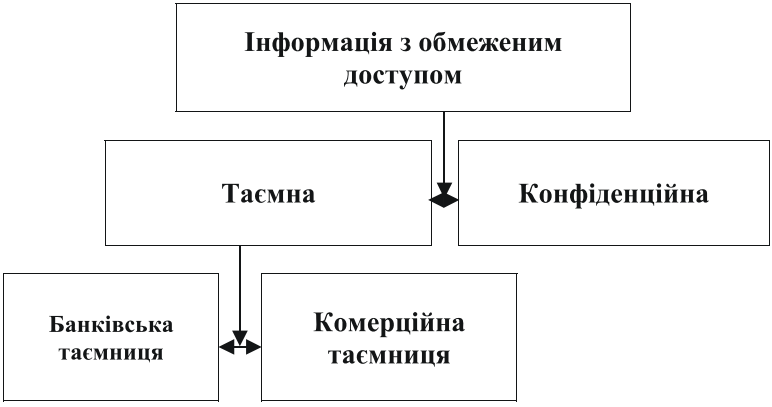
Додаток Б.4.

Класифікація банківської інформації



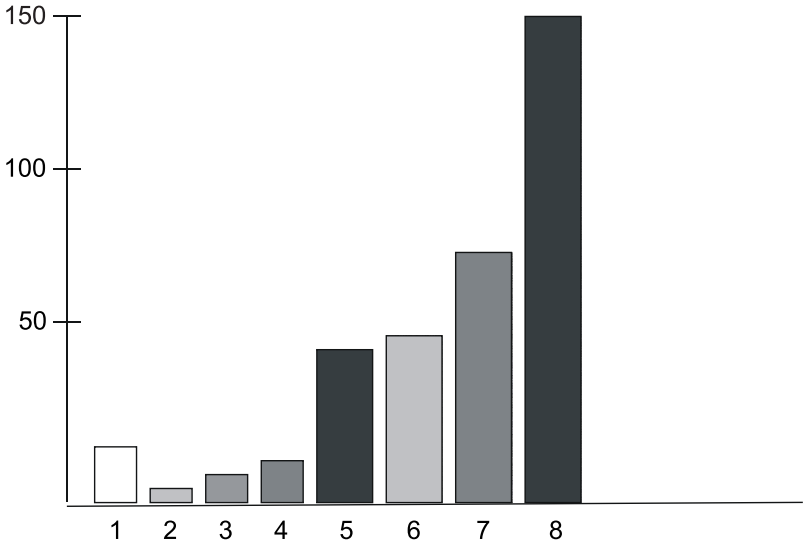
Додаток Б.5.
[92]

Структура банківської інформації з обмеженим доступом



Додаток Б.6.

Запити державних органів про надання інформації у 1996 – 1998 рр. *

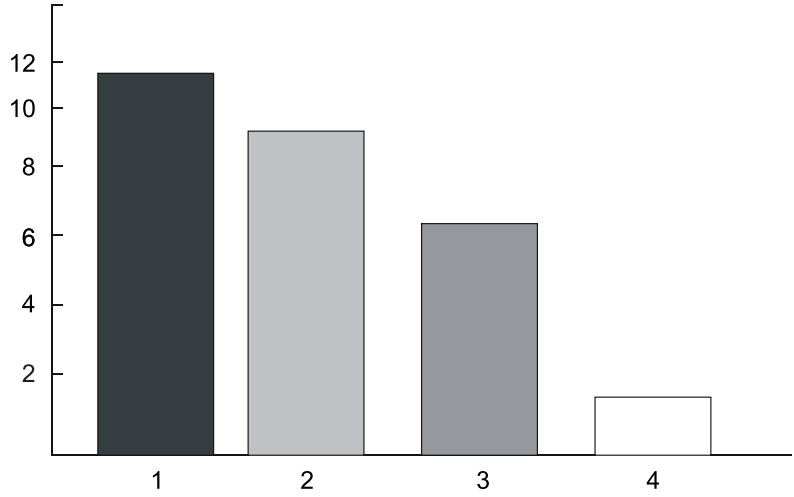


1 – Інші організації
2 – Страхові органи
3 – Судові органи
4 – Антимонопольний комітет
5 – СБУ
6 – Прокуратура
7 – ДПА
8 – МВС

* За даними М.І. Зубок, Л.В. Ніколаєва [92, с. 34].

Додаток Б.7.

Незаконне отримання інформації з обмеженим доступом * [28]



1 – ЗМІ
2 – Конкуренти
3 – Працівники банку
4 – Консультанти

* За даними одного з українських банків [28,с. 37].

Додаток Б.8.

Таблиця показників економічної злочинності в Україні в період становлення державності *

Показники	Роки			
	1990	1995	1996	1997
Кількість випадків шахрайства з фінансовими ресурсами	-	1129	1167	1752
Кількість випадків хабарництва	999	1860	1905	2216
Кількість випадків виготовлення або збуту підроблених грошей чи цінних паперів	22	1894	2816	3646
Кількість виявлених злочинів у фінансово-кредитній системі	-	-	3721	6227
Кількість виявлених злочинів у сфері зовнішньо - економічної діяльності	-	-	859	1245

* За даними О.Г. Данільяна, О.П. Дзьобань, М.І. Панова [81,с. 53].

Додаток В.1

КОНСТИТУЦІЯ УКРАЇНИ
ВИТЯГ

Розділ IV
ВЕРХОВНА РАДА УКРАЇНИ

Стаття 85. До повноважень Верховної Ради України належить:

14) затвердження рішень про надання Україною позик і економічної допомоги іноземним державам та міжнародним організаціям, а також про одержання Україною від іноземних держав, банків і міжнародних фінансових організацій позик, не передбачених Державним бюджетом України, здійснення контролю за їх використанням;

18) призначення на посаду та звільнення з посади Голови Національного банку України за поданням Президента України;

19) призначення та звільнення половини складу Ради Національного банку України;

Розділ V
ПРЕЗИДЕНТ УКРАЇНИ

Стаття 106. Президент України:

12) призначає половину складу Ради Національного банку України.

Додаток В.2

КРИМІНАЛЬНИЙ КОДЕКСУ УКРАЇНИ ВИТЯГ

Стаття 185. **Крадіжка**

1. Таємне викрадення чужого майна (крадіжка) –

карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років.

2. Крадіжка, вчинена повторно або за попередньою змовою групою осіб, –

карається обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк.

3. Крадіжка, поєднана з проникненням у житло, інше приміщення чи сховище або що завдала значної шкоди потерпілому, –

карається позбавленням волі на строк від трьох до шести років.

4. Крадіжка, вчинена у великих розмірах, –

карається позбавленням волі на строк від п'яти до восьми років.

5. Крадіжка, вчинена в особливо великих розмірах або організованою групою, –

карається позбавленням волі на строк від семи до дванадцяти років з конфіскацією майна.

П р и м і т к а. 1. У статтях 185, 186 та 189–191 повторним визнається злочин, вчинений особою, яка раніше вчинила будь-який із злочинів, передбачених цими статтями або статтями 187, 262 цього Кодексу.

2. У статтях 185, 186, 189 та 190 цього Кодексу значна шкода визнається із врахуванням матеріального становища потерпілого та якщо йому спричинені збитки на суму від ста до двохсот п'ятдесяти неоподатковуваних мінімумів доходів громадян.

3. У статтях 185–191 цього Кодексу у великих розмірах визнається злочин, що вчинений однією особою чи групою осіб на суму, яка в двісті п'ятдесят і більше разів перевищує неоподатковуваний мінімум доходів громадян на момент вчинення злочину.

4. У статтях 185–187 та 189–191 цього Кодексу в особливо великих розмірах визнається злочин, що вчинений однією особою чи групою осіб на суму, яка в шістсот і більше разів перевищує неоподатковуваний мінімум доходів громадян на момент вчинення злочину.

Стаття 190. **Шахрайство**

1. Заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою (шахрайство) –

карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років.

2. Шахрайство, вчинене повторно, або за попередньою змовою групою осіб, або таке, що завдало значної шкоди потерпілому, –

карається штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк від одного до двох років, або обмеженням волі на строк до п'яти років, або позбавленням волі на строк до трьох років.

3. Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки, -

карається позбавленням волі на строк від трьох до восьми років.

4. Шахрайство, вчинене в особливо великих розмірах або організованою групою, –

карається позбавленням волі на строк від п'яти до дванадцяти років з конфіскацією майна.

Стаття 358. **Підроблення документів, печаток, штампів та бланків, їх збут, використання підроблених документів**

1. Підроблення посвідчення або іншого документа, який видається чи посвідчується підприємством, установою, організацією, громадянином-підприємцем, приватним нотаріусом, аудитором чи іншою особою, яка має право видавати чи посвідчувати такі документи, і який надає права або звільняє від обов'язків, з метою використання його як підроблювачем, так і іншою особою, або збут такого документа, а також виготовлення підроблених печаток, штампів чи бланків підприємств, установ чи організацій незалежно від форми власності, а так само інших офіційних печаток, штампів чи бланків з тією самою метою або їх збут –

караються штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

2. Дії, передбачені частиною першою цієї статті, якщо вони вчинені повторно або за попередньою змовою групою осіб, –

караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк.

3. Використання завідомо підробленого документа –

карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або обмеженням волі на строк до двох років.

Стаття 231. **Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю**

Умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей (комерційне шпигунство), а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, –

караються штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років, або позбавленням волі на строк до трьох років.

Стаття 232. **Розголошення комерційної таємниці**

Умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, –

карається штрафом від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

Стаття 222. **Шахрайство з фінансовими ресурсами**

1. Надання громадянином-підприємцем або засновником чи власником суб'єкта господарської діяльності, а також службовою особою суб'єкта господарської діяльності завідомо неправдивої інформації органам державної влади, органам влади Автономної Республіки Крим чи органам місцевого самоврядування, банкам або іншим кредиторам з метою одержання субсидій, субвенцій, дотацій, кредитів чи пільг щодо податків у разі відсутності ознак злочину проти власності –

карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

2. Ті самі дії, якщо вони вчинені повторно або завдали великої матеріальної шкоди, –

караються позбавленням волі на строк від двох до п'яти років із позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

Стаття 366. **Службове підроблення**

1. Службове підроблення, тобто внесення службовою особою до офіційних документів завідомо неправдивих відомостей, інше підроблення документів, а також складання і видача за відомо неправдивих документів –

карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

2. Те саме діяння, якщо воно спричинило тяжкі наслідки, -

карається позбавленням волі на строк від двох до п'яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Додаток В.3

ВИТЯГИ ІЗ ЗАКОНІВ УКРАЇНИ

ЗАКОН УКРАЇНИ
«Про банки і банківську діяльність»
ВИТЯГ

Стаття 73. **Заходи впливу**

У разі порушення банками або іншими особами, які можуть бути об'єктом перевірки Національного банку України відповідно до цього Закону, банківського законодавства, нормативно-правових актів Національного банку України або здійснення ризикових операцій, які загрожують інтересам вкладників чи інших кредиторів банку, Національний банк України адекватно вчиненому порушенню має право застосувати заходи впливу, до яких відносяться:

1) письмове застереження щодо припинення порушення та вжиття необхідних заходів для виправлення ситуації, зменшення невиправданих витрат банку, обмеження невиправдано високих процентних виплат за залученими коштами, зменшення чи відчуження неефективних інвестицій;

2) скликання загальних зборів учасників, спостережної ради банку, правління (ради директорів) банку для прийняття програми фінансового оздоровлення банку або плану реорганізації банку;

3) укладення письмової угоди з банком, за якою банк чи визначена угодою особа зобов'язується вжити заходів для усунення порушень, поліпшення фінансового стану банку тощо;

4) видати розпорядження щодо:

а) зупинення виплати дивідендів чи розподілу капіталу в будь-якій іншій формі;

б) встановлення для банку підвищених економічних нормативів;

в) підвищення резервів на покриття можливих збитків за кредитами та іншими активами;

г) обмеження, зупинення чи припинення здійснення окремих видів здійснюваних банком операцій з високим рівнем ризику;

д) заборони надавати бланкові кредити;

е) накладення штрафів на:

керівників банків у розмірі до ста неоподатковуваних мінімумів доходів громадян;

банки відповідно до положень, затверджених Правлінням Національного банку України, але у розмірі не більше одного відсотка від суми зареєстрованого статутного фонду;

є) тимчасової, до усунення порушення, заборони власнику істотної участі в банку використовувати право голосу придбаних акцій (паїв) у разі грубого чи систематичного порушення ним вимог цього Закону або нормативно-правових актів Національного банку України;

ж) тимчасового, до усунення порушення, відсторонення посадової особи банку від посади у разі грубого чи систематичного порушення цією особою вимог цього Закону або нормативно-правових актів Національного банку України;

з) реорганізації банку;

и) призначення тимчасової адміністрації.

У разі порушення цього Закону чи нормативно-правових актів Національного банку України, що спричинило значну втрату активів або доходів, і настанні ознак неплатоспроможності банку Національний банк України має право відкликати ліцензію та ініціювати процедуру ліквідації банку згідно з положеннями цього Закону.

Якщо в діях керівника банку або фізичної особи чи представника юридичної особи – власника істотної участі, якій пред'явлено обвинувачення у вчиненні злочину, не встановлено складу злочину, але має місце порушення вимог цього Закону або нормативно-правових актів Національного банку України або якщо таку особу визнано винною у вчиненні корисливого злочину із призначенням покарання без позбавлення волі, Національний банк України має право видати банку розпорядження про звільнення такої особи з посади або заборону користуватися правом голосу придбаних акцій (паїв).

Особу, яку на підставі розпорядження Національного банку України було відсторонено від посади або якій тимчасово заборонено користуватися правом голосу придбаних акцій (паїв), може бути поновлено на посаді або відновлено у використанні права голосу придбаних акцій (паїв) лише на підставі попереднього дозволу Національного банку України.

Рішення Національного банку України щодо призначення тимчасової адміністрації є виконавчим документом.

Глава 11
ЗАПОБІГАННЯ ТА ПРОТИДІЯ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЮ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Стаття 63. **Запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом**

Банки зобов'язані розробляти, впроваджувати та постійно поновлювати правила внутрішнього фінансового моніторингу та програми його

здійснення з урахуванням вимог законодавства про запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом.

Національний банк України при здійсненні нагляду за діяльністю банків не рідше одного разу на рік проводить перевірку банків з питань дотримання ними законодавства, яке регулює відносини у сфері запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом.

Стаття 64. **Обов'язок щодо ідентифікації клієнтів**

Банкам забороняється відкривати та вести анонімні (номерні) рахунки.

Банкам забороняється вступати в договірні відносини з клієнтами – юридичними чи фізичними особами у разі, якщо виникає сумнів стосовно того, що особа виступає не від власного імені.

Банк зобов'язаний ідентифікувати відповідно до законодавства України:

клієнтів, що відкривають рахунки в банку;

клієнтів, які здійснюють операції, що підлягають фінансовому моніторингу;

клієнтів, що здійснюють операції з готівкою без відкриття рахунку на суму, що перевищує еквівалент 50 000 гривень;

осіб, уповноважених діяти від імені зазначених клієнтів.

Рахунок клієнту відкривається та зазначені операції здійснюються лише після проведення ідентифікації особи клієнтів та вжиття заходів відповідно до законодавства, яке регулює відносини у сфері запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом.

Банк має право витребувати, а клієнт зобов'язаний надати документи і відомості, необхідні для з'ясування його особи, суті діяльності, фінансового стану. У разі ненадання клієнтом необхідних документів чи відомостей або умисного подання неправдивих відомостей про себе банк відмовляє клієнту у його обслуговуванні. У разі наявності при здійсненні ідентифікації мотивованої підозри щодо надання клієнтом недостовірної інформації або навмисного подання інформації з метою введення в оману банк має надавати інформацію про фінансові операції клієнта спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу.

Для ідентифікації клієнта – юридичної особи банк має ідентифікувати фізичних осіб, які є власниками цієї юридичної особи, мають прямий або опосередкований вплив на неї та отримують економічну вигоду від її діяльності. У разі якщо юридична особа є господарським товариством, банк має ідентифікувати фізичних осіб, які мають істотну участь у цій юридичній

особі. Клієнт має надавати передбачені законодавством відомості, які витребує банк з метою виконання вимог законодавства, яке регулює відносини у сфері запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом. У разі ненадання таких відомостей клієнтом рахунок не відкривається, а в разі наявності раніше відкритих рахунків банк відмовляє в здійсненні обслуговування. Для ідентифікації і вжиття заходів, достатніх, на думку банку, для підтвердження особи клієнта – юридичної особи та для забезпечення спроможності банку виконувати правила внутрішнього фінансового моніторингу та програми його здійснення, у тому числі щодо виявлення фінансових операцій, що мають сумнівний характер, банк має право витребувати передбачену законодавством інформацію, яка стосується ідентифікації цієї особи та її керівників, у органів державної влади, які здійснюють нагляд та/або контроль за діяльністю цієї юридичної особи, банків, інших юридичних осіб, а також здійснювати передбачені законодавством заходи щодо збору такої інформації з інших джерел. Вказані органи державної влади, банки, інші юридичні особи зобов'язані протягом десяти робочих днів з дня отримання запиту безоплатно надати банку таку інформацію.

Для ідентифікації клієнта – фізичної особи та вжиття заходів, достатніх, на думку банку, для підтвердження його особи, банк має право витребувати інформацію, яка стосується ідентифікації цієї особи, у органів державної влади, банків, інших юридичних осіб, а також здійснювати заходи щодо збору такої інформації про цю особу, яка є необхідною для виконання правил внутрішнього фінансового моніторингу та програм його здійснення, у тому числі щодо виявлення фінансових операцій, що мають сумнівний характер.

Вказані органи державної влади, банки, інші юридичні особи зобов'язані протягом десяти робочих днів з дня отримання запиту безоплатно надати банку таку інформацію.

Ідентифікація клієнта банку не є обов'язковою при здійсненні кожної операції, якщо клієнт був раніше ідентифікований відповідно до вимог законодавства, яке регулює відносини у сфері запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом.

За наявності рішення уповноваженого державного органу про скасування державної реєстрації юридичної особи або державної реєстрації суб'єкта підприємницької діяльності – фізичної особи,

визнання в установленому порядку юридичної особи фіктивною або оголошення фізичної особи померлою чи визнання безвісно відсутньою банк

закриває рахунок такої особи і невідкладно надає інформацію спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу щодо такого рахунку та не перераховує чи іншим шляхом не розпоряджається коштами на цьому рахунку до отримання розпоряджень зазначеного органу. У випадку ненадходження протягом семи робочих днів зазначених розпоряджень або рішення суду стосовно вжиття чи невжиття заходів щодо цих коштів банк вирішує пов'язані з ними питання відповідно до законодавства України.

Стаття 52. **Угоди з пов'язаними з банком особами**

Угоди, що здійснюються з пов'язаними з банком особами (далі – пов'язані особи), не можуть передбачати більш сприятливі умови, ніж угоди, укладені з іншими особами. Угоди, укладені банком із пов'язаними особами на умовах, сприятливіших за звичайні, визнаються судом недійсними з моменту їх укладення.

Більш сприятливими умовами визначаються:

1) прийняття меншого забезпечення виконання зобов'язань, ніж вимагається від інших клієнтів;

2) придбання у пов'язаної особи майна низької якості чи за завищеною ціною;

3) здійснення інвестиції в цінні папери пов'язаної особи, яку банк не здійснив би в інше підприємство;

4) оплата товарів та послуг пов'язаної особи за цінами вищими, ніж звичайні або за таких обставин, коли такі самі товари і послуги іншої особи взагалі не були б придбані.

Банк може укладати угоди з пов'язаними особами, які передбачають нарахування відсотків та комісійних на здійснення банківських операцій, які менші звичайних, та нарахування відсотків за вкладами і депозитами, які більші звичайних, у разі, якщо прибуток банку дозволяє здійснювати це без шкоди для фінансового розвитку банку.

Банку забороняється надавати кредити будь-якій особі для:

погашення цією особою будь-яких зобов'язань перед пов'язаною особою банку;

придбання активів пов'язаної особи банку;

придбання цінних паперів, розміщених чи підписаних пов'язаною особою банку, за винятком продукції, що виробляється цією особою.

Національний банк України може своїм розпорядженням запроваджувати обмеження на суму угод із пов'язаними особами.

Стаття 59. **Арешт, стягнення та зупинення операцій по рахунках**

Арешт на майно або кошти банку, що знаходяться на його рахунках, а так само арешт на кошти та інші цінності юридичних або фізичних осіб, що знаходяться в банку, накладається виключно за санкціонованою прокурором постановою слідчого, за постановою державного виконавця у випадках, передбачених законами України, або за рішенням суду.

Звільнення майна з-під арешту здійснюється за постановою органу, який прийняв рішення про накладення арешту, або за рішенням суду.

Зупинення власних видаткових операцій банку по його рахунках, а так само зупинення видаткових операцій по рахунках юридичних або фізичних осіб здійснюється уповноваженими відповідно до законів України державними органами і виключно у випадках, передбачених законами України.

Забороняється накладати арешт на кореспондентські рахунки банку або зупиняти операції по цих рахунках.

Операції по рахунках можуть бути відновлені органом, який прийняв рішення про їх зупинення, або за рішенням суду.

Стягнення на власні кошти банку, грошові кошти та інші цінності фізичних чи юридичних осіб, що знаходяться у банку, може бути звернене за виконавчими документами, передбаченими законами України.

Рішенням суду про стягнення на кошти, які знаходяться на рахунках юридичних чи фізичних осіб, видаткові операції по яких зупинені уповноваженим органом, підлягають негайному і безумовному виконанню, за винятком випадків введення мораторію відповідно до цього Закону.

ЗАКОН УКРАЇНИ
«Про Національний банк України»
ВИТЯГ

Стаття 4. **Економічна самостійність**

Національний банк є економічно самостійним органом, який здійснює видатки за рахунок власних доходів у межах затвердженого кошторису, а у визначених цим Законом випадках – також за рахунок Державного бюджету України.

Національний банк є юридичною особою, має відокремлене майно, що є об'єктом права державної власності і перебуває у його повному господарському віданні.

Національний банк не відповідає за зобов'язаннями органів державної влади, а органи державної влади не відповідають за зобов'язаннями Національного банку, крім випадків, коли вони добровільно беруть на себе такі зобов'язання.

Національний банк не відповідає за зобов'язаннями інших банків, а інші банки не відповідають за зобов'язаннями Національного банку, крім випадків, коли вони добровільно беруть на себе такі зобов'язання.

Національний банк може відкривати свої установи, філії та представництва в Україні, а також представництва за її межами.

Національний банк, його установи, філії та представництва мають печатку із зображенням Державного Герба України та своїм найменуванням.

Стаття 6. **Основна функція**

Відповідно до Конституції України основною функцією Національного банку є забезпечення стабільності грошової одиниці України.

На виконання своєї основної функції Національний банк сприяє дотриманню стабільності банківської системи, а також, у межах своїх повноважень, – цінової стабільності.

Стаття 7. **Інші функції**

Національний банк виконує такі функції:

1) відповідно до розроблених Радою Національного банку України Основних засад грошово-кредитної політики визначає та проводить грошово-кредитну політику;

2) монопольно здійснює емісію національної валюти України та організує її обіг;

3) виступає кредитором останньої інстанції для банків і організує систему рефінансування;

4) встановлює для банків правила проведення банківських операцій, бухгалтерського обліку і звітності, захисту інформації, коштів та майна;

5) організовує створення та методологічно забезпечує систему грошово-кредитної і банківської статистичної інформації та статистики платіжного балансу;

6) визначає систему, порядок і форми платежів, у тому числі між банками;

7) визначає напрями розвитку сучасних електронних банківських технологій, створює, координує та контролює створення електронних

платіжних засобів, платіжних систем, автоматизації банківської діяльності та засобів захисту банківської інформації;

8) здійснює банківське регулювання та нагляд;

9) веде Державний реєстр банків, здійснює ліцензування банківської діяльності та операцій у передбачених законами випадках;

10) веде офіційний реєстр ідентифікаційних номерів емітентів платіжних карток внутрішньодержавних платіжних систем;

11) здійснює сертифікацію аудиторів, які проводитимуть аудиторську перевірку банків, тимчасових адміністраторів та ліквідаторів банку;

12) складає платіжний баланс, здійснює його аналіз та прогнозування;

13) представляє інтереси України в центральних банках інших держав, міжнародних банках та інших кредитних установах, де співробітництво здійснюється на рівні центральних банків;

14) здійснює відповідно до визначених спеціальним законом повноважень валютне регулювання, визначає порядок здійснення операцій в іноземній валюті, організовує і здійснює валютний контроль за банками та іншими фінансовими установами, які отримали ліцензію Національного банку на здійснення валютних операцій;

15) забезпечує накопичення та зберігання золотовалютних резервів та здійснення операцій з ними та банківськими металами;

16) аналізує стан грошово-кредитних, фінансових, цінових та валютних відносин;

17) організує інкасацію та перевезення банкнот і монет та інших цінностей, видає ліцензії на право інкасації та перевезення банкнот і монет та інших цінностей;

18) реалізує державну політику з питань захисту державних секретів у системі Національного банку;

19) бере участь у підготовці кадрів для банківської системи України;

20) визначає особливості функціонування банківської системи України в разі введення воєнного стану чи особливого періоду, здійснює мобілізаційну підготовку системи Національного банку;

21) здійснює інші функції у фінансово-кредитній сфері в межах своєї компетенції, визначеної законом.

Стаття 51. **Підзвітність**

Національний банк підзвітний Президенту України та Верховній Раді України в межах їх конституційних повноважень.

Підзвітність означає:

1) призначення на посаду та звільнення з посади Голови Національного банку Верховною Радою України за поданням Президента України;

2) призначення та звільнення Президентом України половини складу Ради Національного банку;

3) призначення та звільнення Верховною Радою України половини складу Ради Національного банку;

4) доповідь Голови Національного банку Верховній Раді України про діяльність Національного банку;

5) надання Президенту України та Верховній Раді України двічі на рік інформації про стан грошово-кредитного ринку в державі.

Стаття 52. **Взаємовідносини з Кабінетом Міністрів України**

Національний банк та Кабінет Міністрів України проводять взаємні консультації з питань грошово-кредитної політики, розробки і здійснення загальнодержавної програми економічного та соціального розвитку.

Національний банк на запит Кабінету Міністрів України надає інформацію щодо монетарних процесів.

Кабінет Міністрів України, міністерства та інші центральні органи виконавчої влади на запит Національного банку надають інформацію, що має вплив на стан платіжного балансу.

Національний банк підтримує економічну політику Кабінету Міністрів України, якщо вона не суперечить забезпеченню стабільності грошової одиниці України.

Голова Національного банку або за його дорученням один із його заступників можуть брати участь у засіданнях Кабінету Міністрів України з правом дорадчого голосу.

У засіданнях Правління Національного банку можуть брати участь члени Кабінету Міністрів України з правом дорадчого голосу.

Стаття 53. **Гарантії невтручання**

Не допускається втручання органів законодавчої та виконавчої влади або їх посадових осіб у виконання функцій і повноважень Ради Національного банку чи Правління Національного банку інакше, як в межах, визначених цим Законом.

Стаття 54. **Надання кредитів державі**

Національному банку забороняється надавати прямі кредити як у національній, так і в іноземній валюті на фінансування витрат Державного бюджету України.

Стаття 55. **Мета та сфера банківського нагляду**

Головна мета банківського регулювання і нагляду – безпека та фінансова стабільність банківської системи, захист інтересів вкладників і кредиторів.

Національний банк здійснює функції банківського регулювання і нагляду за діяльністю банків, в межах та порядку, передбачених законодавством України.

Національний банк здійснює постійний нагляд за дотриманням банками, їх підрозділами, афілійованими та спорідненими особами банків на території України та за кордоном, банківськими об'єднаннями, представництвами та філіями іноземних банків в Україні, а також іншими юридичними та фізичними особами банківського законодавства, нормативно-правових актів Національного банку і економічних нормативів. Національний банк не здійснює перевірок і ревізій фінансово-господарської діяльності осіб, зазначених у цій статті.

Стаття 57. **Доступ до інформації**

Для здійснення своїх функцій Національний банк має право безоплатно одержувати від банків, банківських об'єднань та юридичних осіб, які отримали ліцензію Національного банку на здійснення окремих банківських операцій, а також від осіб, стосовно яких Національний банк здійснює наглядову діяльність відповідно до Закону України «Про банки і банківську діяльність», інформацію про їх діяльність та пояснення стосовно отриманої інформації і проведених операцій.

Для підготовки банківської та фінансової статистики, аналізу економічної ситуації Національний банк має право безоплатно отримувати необхідну інформацію від органів державної влади і органів місцевого самоврядування та суб'єктів господарювання усіх форм власності.

Отримана інформація не підлягає розголошенню, за винятком випадків, передбачених законодавством України.

Стаття 59. **Резерви забезпечення ризиків**

Національний банк визначає розміри, порядок формування та використання резервів банків для покриття можливих втрат за кредитами, резервів для покриття валютних, відсоткових та інших ризиків банків.

Резерви для покриття можливих фінансових ризиків, а також фонду гарантування вкладів громадян створюються за рахунок доходу до оподаткування відповідно до законодавства України.

Стаття 63. **Обмеження вимог Національного банку**

Національний банк не має права вимагати від банків виконання операцій та інших дій, не передбачених законами України та нормативними актами Національного банку.

Стаття 64. **Статус працівників Національного банку**

Умови найму, звільнення, оплати праці, надання відпусток, службові обов'язки та права, система дисциплінарних стягнень, питання соціального захисту службовців Національного банку визначаються Законом України «Про державну службу».

Працівниками Національного банку є службовці та обслуговуючий персонал Національного банку. Службовцями вважаються особи, які безпосередньо беруть участь у виконанні функцій Національного банку та займають посади, передбачені штатним розписом.

Правління Національного банку визначає перелік посад працівників, трудовий договір з якими укладається у формі контракту.

Службовці Національного банку є державними службовцями, і до них застосовуються норми Закону України «Про державну службу», якщо цей Закон не встановлює іншого.

Питання функціонування державної служби у Національному банку та класифікації посад вирішує Правління Національного банку відповідно до законодавства України.

Ранги державних службовців Національного банку, що відповідають посадам першої категорії, присвоюються Президентом України. Інші ранги присвоюються Головою Національного банку.

До складу обслуговуючого персоналу Національного банку входять працівники, обов'язки яких безпосередньо не пов'язані із виконанням функцій Національного банку.

Розмір оплати праці службовців Національного банку встановлюється Правлінням Національного банку відповідно до положень Закону України «Про державну службу».

Розмір оплати праці обслуговуючого персоналу Національного банку встановлюється Правлінням Національного банку відповідно до норм законодавства про оплату праці.

Стаття 65. **Заборонена діяльність**

Голова Національного банку, його заступники, члени Правління Національного банку та інші службовці Національного банку згідно із переліком посад, затвердженим Правлінням Національного банку, не можуть бути народними депутатами України, членами Уряду України, займатися підприємницькою діяльністю, виконувати роботу за сумісництвом, крім викладацької, наукової та іншої творчої діяльності.

Службовцям Національного банку забороняється входити до керівних органів та бути акціонерами банків.

Голові Національного банку, його заступникам, членам Правління Національного банку та іншим службовцям Національного банку забороняється отримувати позики від будь-яких інших кредитних установ, за винятком Національного банку.

Стаття 66. **Збереження таємниці**

Службовцям Національного банку забороняється розголошувати інформацію, що становить державну таємницю, банківську таємницю або

іншу конфіденційну інформацію, яка стала відома їм у зв'язку з виконанням службових обов'язків, і в разі припинення роботи в Національному банку, крім випадків, передбачених законодавством України.

Президент України Л. КУЧМА
м. Київ, 20 травня 1999 року № 679-XIV

ЗАКОН УКРАЇНИ
«Про організаційно-правові основи боротьби з організованою злочинністю»
ВИТЯГ

Стаття 12. **Права спеціальних підрозділів по боротьбі з організованою злочинністю органів внутрішніх справ, Служби безпеки України та їх співробітників**

1. Спеціальні підрозділи по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України та їх співробітники мають права, передбачені законами України «Про міліцію», «Про Службу безпеки України», «Про оперативно-розшукову діяльність», цим Законом та іншими законодавчими актами України.

2. При здійсненні заходів боротьби з організованою злочинністю спеціальним підрозділам по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України надаються повноваження:

а) заводити оперативно-розшукові справи. Постанова про заведення справи затверджується начальником спеціального підрозділу;

б) на письмову вимогу керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю одержувати від банків, а також кредитних, митних, фінансових та інших установ, підприємств, організацій (незалежно від форм власності) інформацію і документи про операції, рахунки, вклади, внутрішні та зовнішні економічні угоди фізичних і юридичних осіб. Отримання від банків інформації, яка містить банківську таємницю, здійснюється у порядку та обсязі, встановлених Законом України «Про банки і банківську діяльність». Документи та інформація повинні бути подані негайно, а якщо це неможливо – не пізніш як протягом 10 діб;

в) залучати до проведення перевірок, ревізій та експертиз кваліфікованих спеціалістів установ, організацій контрольних і фінансових органів;

г) одержувати інформацію з автоматизованих інформаційних і довідкових систем та банків даних, створюваних Верховним Судом України, Генеральною прокуратурою України, Антимонопольним комітетом України, Фондом державного майна України, міністерствами, відомствами, іншими державними органами України;

д) в разі одержання фактичних даних про організовану злочинну діяльність для їх перевірки витребувати та одержувати від державних органів, об'єднань громадян, підприємств, установ, організацій (незалежно від форм власності) інформацію і документи. Витребовувані документи та інформація повинні бути подані негайно або не пізніш як протягом 10 діб.

3. За матеріалами оперативно-розшукової діяльності та кримінальних справ спеціальні підрозділи по боротьбі з організованою злочинністю мають право подавати до суду заяви про скасування реєстрації і припинення діяльності суб'єктів підприємництва, а також за наявності підстав, передбачених Законом, подавати до суду позови про визнання недійсними угод у порядку, встановленому законодавством України.

4. При здійсненні боротьби з організованою злочинністю співробітники спеціальних підрозділів органів внутрішніх справ і Служби безпеки України мають право:

а) за письмовим розпорядженням керівника відповідного спеціального підрозділу входити за службовими посвідченнями на територію, у приміщення, склади та сховища підприємств, організацій і установ (крім іноземних, дипломатичних представництв), незалежно від їх відомчої належності та форм власності, у пункти пропуску через державний кордон України та митниці, а також у виробничі приміщення громадян, які займаються підприємницькою діяльністю;

б) за постановою та з санкції відповідного прокурора по нагляду за виконанням законів спеціальними підрозділами по боротьбі з організованою злочинністю, а у невідкладних випадках – з наступним повідомленням прокурора протягом доби в разі загрози знищення, приховування або втрати предметів чи документів, які можуть бути використані у розкритті та розслідуванні злочинної діяльності, на строк до 10 діб опечатувати архіви, каси, приміщення (за винятком жилих) чи інші сховища, брати їх під охорону, накладати арешт на грошові кошти та інші цінності фізичних та юридичних осіб, вилучати предмети і документи із складанням відповідного акта. Копії акта вручаються громадянину чи представнику підприємства, установи, організації.

5. Оперативні управління, відділи та відділення спеціальних підрозділів мають повноваження органу дізнання. Спеціальні підрозділи по боротьбі з організованою злочинністю можуть порушувати і розслідувати, передавати через відповідного прокурора по нагляду за виконанням законів спеціальними підрозділами за підслідністю в інші органи внутрішніх справ і Служби безпеки України кримінальні справи про виявлені ними злочини, у такому ж порядку витребувати і приймати від них до свого провадження кримінальні справи про злочини, вчинені організованими злочинними угрупованнями. Питання вирішення спорів про підслідність зазначених

кримінальних справ регулюються цим Законом і Кримінально-процесуальним кодексом України.

Президент України Л.КРАВЧУК
м. Київ, 30 червня 1993 року № 3341-XII

ЗАКОН УКРАЇНИ
«Про внесення змін до деяких законів України з питань запобігання використанню банків та інших фінансових установ з метою легалізації (відмивання) доходів, одержаних злочинним шляхом»
ВИТЯГ

Глава 11
ЗАПОБІГАННЯ ТА ПРОТИДІЯ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЮ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Стаття 63. Запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом

Банки зобов'язані розробляти, впроваджувати та постійно поновлювати правила внутрішнього фінансового моніторингу та програми його здійснення з урахуванням вимог законодавства про запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом.

Національний банк України при здійсненні нагляду за діяльністю банків не рідше одного разу на рік проводить перевірку банків з питань дотримання ними законодавства, яке регулює відносини у сфері запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом.

2. Статтю 18 Закону України «Про фінансові послуги та державне регулювання ринків фінансових послуг» викласти у такій редакції:

«Стаття 18. Запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом

Фінансовим установам під час здійснення (надання) фінансових послуг забороняється вступати в договірні відносини з анонімними особами, відкривати та вести анонімні (номерні) рахунки.

Фінансовим установам забороняється вступати в договірні відносини з клієнтами – юридичними чи фізичними особами у разі, якщо виникає сумнів стосовно того, що особа виступає не від власного імені.

3. У Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом»:

1) частину третю статті 8 викласти в такій редакції:

«Суб'єкти первинного фінансового моніторингу, їх посадові особи та інші працівники не несуть дисциплінарну, адміністративну, цивільно-правову та кримінальну відповідальність за надання Уповноваженому органу інформації про фінансову операцію, якщо вони діяли в межах цього Закону, навіть якщо такими діями заподіяно шкоду юридичним або фізичним особам, та за інші дії, пов'язані з виконанням цього Закону»;

2) в абзаці першому статті 11 слова «якщо сума, на яку вона проводиться, при безготівкових розрахунках дорівнює чи перевищує 300 000 гривень або дорівнює чи перевищує суму в іноземній валюті, еквівалентну 300000 гривень, при розрахунках готівкою дорівнює чи перевищує 100 000 гривень або дорівнює чи перевищує суму в іноземній валюті, еквівалентну 100000 гривень» замінити словами «якщо сума, на яку вона проводиться, дорівнює чи перевищує 80000 гривень або дорівнює чи перевищує суму в іноземній валюті, еквівалентну 80000 гривень»;

3) доповнити статтею 13^1 такого змісту:

«Стаття 13^1. **Політична незалежність Уповноваженого органу.**

Керівник Уповноваженого органу призначається і звільняється з посади у встановленому законодавством порядку.

Використання Уповноваженого органу в партійних, групових чи особистих інтересах не допускається.

Діяльність партій, рухів та інших громадських об'єднань, що мають політичні цілі, в Уповноваженому органі забороняється.

На період служби чи роботи за трудовим договором членство посадових і службових осіб Уповноваженого органу у таких об'єднаннях зупиняється.

Як виняток дозволяється членство працівників, які уклали трудовий договір з Уповноваженим органом, у професійних спілках».

4. Абзац другий частини першої статті 306 Кримінального кодексу України (в редакції Закону України від 16 січня 2003 року N 430-IV) викласти в такій редакції:

«караються позбавленням волі на строк від п'яти до дванадцяти років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років з конфіскацією коштів або іншого майна, одержаних злочинним шляхом, та з конфіскацією майна».

4. Банки зобов'язані протягом одного місяця з дня набрання чинності цим Законом закрити анонімні валютні та кодовані рахунки у порядку, встановленому Національним банком України.

Президент України Л. КУЧМА

м. Київ, 6 лютого 2003 року N 485-IV

ЗАКОН УКРАЇНИ
«Про інформацію»
ВИТЯГ

Стаття 9. **Право на інформацію**

Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України.

Стаття 30. **Інформація з обмеженим доступом**

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденціальну і таємну. Конфіденціальна 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.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденціальної, та встановлюють для неї систему (способи) захисту.

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про цю інформацію.

Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених цим Законом.

Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист.

Президент України Л. КРАВЧУК
м. Київ, 2 жовтня 1992 року
№ 2657-XII

ЗАКОН УКРАЇНИ
«Про державну таємницю»
ВИТЯГ

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 3. **Сфера дії Закону**

Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші органи державної влади, Верховну Раду Автономної Республіки Крим, Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі – органи державної влади, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.

Передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом. У разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, установлено інші, ніж передбачені цим Законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору України.

Стаття 4. **Державна політика щодо державної таємниці**

Державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України.

Стаття 5. **Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці**

Президент України, забезпечуючи національну безпеку, видає укази та розпорядження з питань охорони державної таємниці, віднесених цим Законом та іншими законами до його повноважень.

Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці.

Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері охорони державної таємниці.

Центральні та місцеві органи виконавчої влади, Рада міністрів Автономної Республіки Крим та органи місцевого самоврядування здійснюють державну політику у сфері охорони державної таємниці в межах своїх повноважень, передбачених законом.

Спеціально уповноваженим органом державної влади у сфері забезпечення охорони державної таємниці є Служба безпеки України.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

Розділ II
ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 8. **Інформація, що може бути віднесена до державної таємниці**

До державної таємниці у порядку, встановленому цим Законом, відноситься інформація:

2) у сфері економіки, науки і техніки:

про мобілізаційні плани і мобілізаційні потужності господарства України, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, про загальні обсяги поставок, відпуску, закладення, освіження, розміщення і фактичні запаси державного резерву;

про використання транспорту, зв'язку, потужностей інших галузей та об'єктів інфраструктури держави в інтересах забезпечення її безпеки;

про плани, зміст, обсяг, фінансування та виконання державного замовлення для забезпечення потреб оборони та безпеки;

про плани, обсяги та інші найважливіші характеристики добування, виробництва та реалізації окремих стратегічних видів сировини і продукції;

про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей, операції, пов'язані з виготовленням грошових знаків і цінних паперів, їх зберіганням, охороною і захистом від підроблення, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, на базі яких можуть бути створені прогресивні технології, нові види виробництва, продукції та технологічних процесів, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

Стаття 12. **Звід відомостей, що становлять державну таємницю**

Звід відомостей, що становлять державну таємницю, формує та публікує в офіційних виданнях Служба безпеки України на підставі рішень державних експертів з питань таємниць.

Зміни до Зводу відомостей, що становлять державну таємницю, публікуються не пізніше трьох місяців з дня одержання Службою безпеки України відповідного рішення чи висновку державного експерта з питань таємниць.

Зразки форм рішень (висновків) державних експертів з питань таємниць, порядок та механізм формування Зводу відомостей, що становлять державну таємницю, і його опублікування визначаються Кабінетом Міністрів України.

На підставі та в межах Зводу відомостей, що становлять державну таємницю, з метою конкретизації та систематизації даних про секретну інформацію органи державної влади створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю. Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану із державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Такі переліки погоджуються із Службою безпеки України, затверджуються державними експертами з питань таємниць та реєструються у Службі безпеки України.

Розгорнуті переліки відомостей, що становлять державну таємницю, не можуть суперечити Зводу відомостей, що становлять державну таємницю.

У разі включення до Зводу відомостей, що становлять державну таємницю, або до розгорнутих переліків цих відомостей інформації, яка не відповідає категоріям і вимогам, передбаченим статтею 8 цього Закону, або порушення встановленого порядку віднесення інформації до державної таємниці заінтересовані громадяни та юридичні особи мають право оскаржити відповідні рішення до суду. З метою недопущення розголошення державної таємниці судовий розгляд скарг може проводитися в закритих засіданнях відповідно до закону.

Розділ IV
ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 18. **Основні організаційно-правові заходи щодо охорони державної таємниці**

З метою охорони державної таємниці впроваджуються:

єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

дозвільний порядок провадження органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;

обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

особливості здійснення органами державної влади їх функцій щодо органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

режим секретності органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

спеціальний порядок допуску та доступу громадян до державної таємниці;

технічний та криптографічний захисти секретної інформації.

Стаття 19. **Єдині вимоги до матеріальних носіїв секретної інформації**

Єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації встановлюються Кабінетом Міністрів України.

Стаття 20. **Дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, та режим секретності**

Органи державної влади, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею...

Стаття 21. **Режимно-секретні органи**

В органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням створюються на правах окремих структурних підрозділів режимно-секретні органи (далі – РСО)...

Стаття 22. **Допуск громадян до державної таємниці**

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:

форма 1 – для роботи з секретною інформацією, що має ступені секретності «особливої важливості», «цілком таємно» та «таємно»;

форма 2 – для роботи з секретною інформацією, що має ступені секретності «цілком таємно» та «таємно»;

форма 3 – для роботи з секретною інформацією, що має ступінь секретності «таємно».

Стаття 27. **Доступ громадян до державної таємниці**

Доступ до державної таємниці надається дієздатним громадянам України, яким надано допуск до державної таємниці та які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання.

Стаття 28. **Обов'язки громадянина щодо збереження державної таємниці**

Громадянин, якому надано допуск до державної таємниці, зобов'язаний:

не допускати розголошення будь-яким способом державної таємниці, яка йому довірена або стала відомою у зв'язку з виконанням службових обов'язків;

не брати участі в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, встановленому законом;

не сприяти іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у

провадженні діяльності, що завдає шкоди інтересам національної безпеки України;

виконувати вимоги режиму секретності;

повідомляти посадових осіб, які надали йому допуск до державної таємниці, та відповідні режимно-секретні органи про виникнення обставин, передбачених статтею 23 цього Закону, або інших обставин, що перешкоджають збереженню довіреної йому державної таємниці, а також про свій виїзд з України;

додержуватися інших вимог законодавства про державну таємницю.

Стаття 29. **Обмеження прав у зв'язку з допуском та доступом до державної таємниці**

Громадянин, якому було надано допуск та доступ до державної таємниці у порядку, встановленому законодавством, і який реально був обізнаний з нею, може бути обмежений у праві виїзду на постійне місце проживання в іноземну державу до розсекречування відповідної інформації, але не більш як на п'ять років з часу припинення діяльності, пов'язаної з державною таємницею.

Не обмежується виїзд у держави, з якими Україна має міжнародні договори, що передбачають такий виїзд і згода на обов'язковість яких надана Верховною Радою України.

На громадянина також поширюються обмеження свободи інформаційної діяльності, що випливають з цього Закону.

Розділ V
КОНТРОЛЬ ЗА ЗАБЕЗПЕЧЕННЯМ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА НАГЛЯД ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 37. **Контроль за забезпеченням охорони державної таємниці**

Керівники органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони державної таємниці.

Органи державної влади, органи місцевого самоврядування, підприємства, установи і організації, що розміщують замовлення у підрядників, зобов'язані контролювати стан охорони державної таємниці, яка була передана підрядникам у зв'язку з виконанням замовлення.

Органи державної влади, яким рішенням державного експерта з питань таємниць було надано право вирішувати питання про доступ органів державної влади, органів місцевого самоврядування, підприємств, установ,

організацій до конкретної секретної інформації, зобов'язані контролювати стан охорони державної таємниці в усіх органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, які виконують роботи, пов'язані з відповідною державною таємницею, або зберігають матеріальні носії зазначеної секретної інформації.

Контроль за додержанням законодавства про державну таємницю в системі Служби безпеки України здійснюється відповідно до Закону України «Про Службу безпеки України».

Служба безпеки України має право контролювати стан охорони державної таємниці в усіх органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, а також у зв'язку з виконанням цих повноважень одержувати безоплатно від них інформацію з питань забезпечення охорони державної таємниці. Висновки Служби безпеки України, викладені в актах офіційних перевірок за результатами контролю стану охорони державної таємниці, є обов'язковими для виконання посадовими особами підприємств, установ та організацій незалежно від їх форм власності.

Розділ VI
ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 39. **Відповідальність за порушення законодавства про державну таємницю**

Посадові особи та громадяни, винні у:

розголошенні державної таємниці;

втраті документів та інших матеріальних носіїв секретної інформації;

недодержанні встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

засекречуванні інформації, зазначеної у частинах третій і четвертій статті 8 цього Закону;

навмисному невіднесенні до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України, а також необґрунтованому заниженні ступеня секретності або необґрунтованому розсекречуванні секретної інформації;

безпідставному засекречуванні інформації;

наданні грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненаданні грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставному скасуванні чи зниженні грифа секретності матеріальних носіїв секретної інформації;

порушенні встановленого законодавством порядку надання допуску та доступу до державної таємниці;

порушенні встановленого законодавством режиму секретності та невиконанні обов'язків щодо збереження державної таємниці;

невжитті заходів щодо забезпечення охорони державної таємниці та незабезпеченні контролю за охороною державної таємниці;

провадженні діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщенні державних замовлень на виконання робіт, доведенні мобілізаційних завдань, пов'язаних з державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

недодержанні вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними;

невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочення її технічними каналами, -

несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом.

Президент України Л. КРАВЧУК

м. Київ, 21 січня 1994 року № 3855-XII

ЗАКОН УКРАЇНИ
«Про підприємства в Україні»
ВИТЯГ

Стаття 30. Комерційна таємниця підприємства

1. Під комерційною таємницею підприємства маються на увазі відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам.

2. Склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства. Відомості, які не можуть становити комерційної таємниці, визначаються Кабінетом Міністрів України.

3. Відповідальність за розголошення відомостей, які становлять комерційну таємницю підприємства, і порядок охорони таких відомостей встановлюються законодавчими актами України.

Голова Верховної Ради України Л. КРАВЧУК
м. Київ, 27 березня 1991 року № 887-XII

ЗАКОН УКРАЇНИ
«Про захист інформації в автоматизованих» системах
ВИТЯГ

Стаття 6. **Доступ до інформації**

Доступ до інформації, яка зберігається, обробляється і передається в АС, здійснюється лише згідно з правилами розмежування доступу, встановленими власником інформації чи уповноваженою ним особою.

Без дозволу власника доступ до інформації, яка обробляється в АС, здійснюється лише у випадках, передбачених чинним законодавством.

Президент України Л. КУЧМА
м. Київ, 5 липня 1994 року № 80/94-ВР

ЗАКОН УКРАЇНИ
«Про захист від недобросовісної конкуренції»
ВИТЯГ

Стаття 16. **Неправомірне збирання комерційної таємниці**

Неправомірним збиранням комерційної таємниці вважається добування протиправним способом відомостей, що відповідно до законодавства України становлять комерційну таємницю, якщо це завдало чи могло завдати шкоди господарюючому суб'єкту (підприємцю).

Стаття 17. **Розголошення комерційної таємниці**

Розголошенням комерційної таємниці є ознайомлення іншої особи без згоди особи, уповноваженої на те, з відомостями, що відповідно до чинного законодавства України становлять комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків, якщо це завдало чи могло завдати шкоди господарюючому суб'єкту (підприємцю).

Стаття 18. **Схилення до розголошення комерційної таємниці**

Схиленням до розголошення комерційної таємниці є спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням службових обов'язків відомості, що відповідно до законодавства України становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди господарюючому суб'єкту (підприємцю).

Стаття 19. **Неправомірне використання комерційної таємниці**

Неправомірним використанням комерційної таємниці є впровадження у виробництво або врахування під час планування чи здійснення підприємницької діяльності без дозволу уповноваженої на те особи неправомірно здобутих відомостей, що становлять відповідно до законодавства України комерційну таємницю.

Президент України Л. КУЧМА
м. Київ, 7 червня 1996 року № 236/96-ВР

ЗАКОН УКРАЇНИ
«Про аудиторську діяльність»
ВИТЯГ

Стаття 3. **Аудиторська діяльність**

Аудиторська діяльність включає в себе організаційне і методичне забезпечення аудиту, практичне виконання аудиторських перевірок (аудит) та надання інших аудиторських послуг.

Аудиторські послуги можуть надаватись у формі аудиторських перевірок (аудиту) та пов'язаних з ними експертиз, консультацій з питань бухгалтерського обліку, звітності, оподаткування, аналізу фінансово-господарської діяльності та інших видів економіко-правового забезпечення підприємницької діяльності фізичних та юридичних осіб.

Прибуток (доход) від аудиторської діяльності оподатковується згідно з чинним законодавством.

Стаття 4. **Аудит**

Аудит – це перевірка публічної бухгалтерської звітності, обліку, первинних документів та іншої інформації щодо фінансово-господарської діяльності суб'єктів господарювання з метою визначення достовірності їх звітності, обліку, його повноти і відповідності чинному законодавству та встановленим нормативам.

Аудит здійснюється незалежними особами (аудиторами), аудиторськими фірмами, які уповноважені суб'єктами господарювання на його проведення.

Аудит може проводитись з ініціативи господарюючих суб'єктів, а також у випадках, передбачених чинним законодавством (обов'язковий аудит).

Затрати на проведення аудиту відносяться на собівартість товару (продукції, послуг).

Стаття 22. **Права аудиторів і аудиторських фірм**

Аудитори і аудиторські фірми України мають право:

1) самостійно визначати форми і методи аудиту на підставі чинного законодавства, існуючих норм і стандартів, умов договору із замовником, професійних знань та досвіду;

2) отримувати необхідні документи, які мають відношення до предмету перевірки і знаходяться як у замовника, так і у третіх осіб.

Треті особи, які мають у своєму розпорядженні документи стосовно предмету перевірки, зобов'язані надати їх на вимогу аудитора (аудиторської фірми). Зазначена вимога повинна бути офіційно засвідчена замовником;

3) отримувати необхідні пояснення в письмовій чи усній формі від керівництва та працівників замовника;

4) перевіряти наявність майна, грошей, цінностей, вимагати від керівництва господарюючого суб'єкта проведення контрольних оглядів, замірів виконаних робіт, визначення якості продукції, щодо яких здійснюється перевірка документів;

5) залучати на договірних засадах до участі в перевірці фахівців різного профілю.

Стаття 23. **Обов'язки аудиторів і аудиторських фірм**

Аудитори і аудиторські фірми зобов'язані:

1) належним чином надавати аудиторські послуги, перевіряти стан бухгалтерського обліку і звітності замовника, їх достовірність, повноту і відповідність чинному законодавству та встановленим нормативам;

2) повідомляти власників, уповноважених ними осіб, замовників про виявлені під час проведення аудиту недоліки ведення бухгалтерського обліку і звітності;

3) зберігати в таємниці інформацію, отриману при проведенні аудиту та виконанні інших аудиторських послуг. Не розголошувати відомості, що становлять предмет комерційної таємниці, і не використовувати їх у своїх інтересах або в інтересах третіх осіб;

4) відповідати перед замовником за порушення умов договору відповідно до чинних законодавчих актів України;

5) обмежувати свою діяльність наданням аудиторських послуг та іншими видами робіт, які мають безпосереднє відношення до надання аудиторських послуг у формі консультацій, перевірок або експертиз.

Президент України Л. КРАВЧУК
м. Київ, 22 квітня 1993 року № 3125-XII

ЗАКОН УКРАЇНИ
«Про основи національної безпеки України»
ВИТЯГ

Стаття 3. **Об'єкти національної безпеки**

Об'єктами національної безпеки є:

людина і громадянин – їхні конституційні права і свободи;

суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси;

держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Стаття 4. **Суб'єкти забезпечення національної безпеки**

Суб'єктами забезпечення національної безпеки є:

Президент України; Верховна Рада України; Кабінет Міністрів України;

Рада національної безпеки і оборони України;

міністерства та інші центральні органи виконавчої влади;

Національний банк України; суди загальної юрисдикції; прокуратура України;

місцеві державні адміністрації та органи місцевого самоврядування;

Збройні Сили України, Служба безпеки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України;

громадяни України, об'єднання громадян.

Стаття 7. **Загрози національним інтересам і національній безпеці України**

На сучасному етапі основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві є:

в економічній сфері:

істотне скорочення внутрішнього валового продукту, зниження інвестиційної та інноваційної активності і науково-технічного та технологічного потенціалу, скорочення досліджень на стратегічно важливих напрямах інноваційного розвитку;

ослаблення системи державного регулювання і контролю у сфері економіки;

нестабільність у правовому регулюванні відносин у сфері економіки, в тому числі фінансової (фіскальної) політики держави; відсутність ефективної програми запобігання фінансовим кризам; зростання кредитних ризиків;

критичний стан основних виробничих фондів у провідних галузях промисловості, агропромисловому комплексі, системах життєзабезпечення; загострення проблеми підтримання в належному технічному стані ядерних об'єктів на території України;

недостатні темпи відтворювальних процесів та подолання структурної деформації в економіці;

критична залежність національної економіки від кон'юнктури зовнішніх ринків, низькі темпи розширення внутрішнього ринку;

нераціональна структура експорту з переважно сировинним характером та низькою питомою вагою продукції з високою часткою доданої вартості;

велика боргова залежність держави, критичні обсяги державних зовнішнього і внутрішнього боргів;

небезпечне для економічної незалежності України зростання частки іноземного капіталу у стратегічних галузях економіки;

неефективність антимонопольної політики та механізмів державного регулювання природних монополій, що ускладнює створення конкурентного середовища в економіці;

критичний стан з продовольчим забезпеченням населення;

неефективність використання паливно-енергетичних ресурсів, недостатні темпи диверсифікації джерел їх постачання та відсутність активної політики енергозбереження, що створює загрозу енергетичній безпеці держави;

«тінізація» національної економіки;

переважання в діяльності управлінських структур особистих, корпоративних, регіональних інтересів над загальнонаціональними;

у соціальній та гуманітарній сферах:

невідповідність програм реформування економіки країни і результатів їх здійснення визначеним соціальним пріоритетам;

неефективність державної політики щодо підвищення трудових доходів громадян, подолання бідності та збалансування продуктивної зайнятості працездатного населення;

криза системи охорони здоров'я і соціального захисту населення і, як наслідок, небезпечне погіршення стану здоров'я населення; поширення наркоманії, алкоголізму, соціальних хвороб;

загострення демографічної кризи;

зниження можливостей здобуття якісної освіти представниками бідних прошарків суспільства;

прояви моральної та духовної деградації суспільства;

зростання дитячої та підліткової бездоглядності, безпритульності, бродяжництва.

Стаття 8. **Основні напрями державної політики з питань національної безпеки**

Основними напрямами державної політики з питань національної безпеки України є:

в економічній сфері:

забезпечення умов для сталого економічного зростання та підвищення конкурентоспроможності національної економіки;

прискорення прогресивних структурних та інституціональних змін в економіці, поліпшення інвестиційного клімату, підвищення ефективності інвестиційних процесів; стимулювання випереджувального розвитку наукоємних високотехнологічних виробництв;

вдосконалення антимонопольної політики; створення ефективного механізму державного регулювання природних монополій;

подолання «тінізації» економіки через реформування податкової системи, оздоровлення фінансово-кредитної сфери та припинення відпливу капіталів за кордон, зменшення позабанківського обігу грошової маси;

забезпечення збалансованого розвитку бюджетної сфери, внутрішньої і зовнішньої захищеності національної валюти, її стабільності, захисту інтересів вкладників, фінансового ринку;

здійснення виваженої політики внутрішніх та зовнішніх запозичень;

забезпечення енергетичної безпеки на основі сталого функціонування і розвитку паливно-енергетичного комплексу, в тому числі послідовного і активного проведення політики енергозбереження та диверсифікації джерел енергозабезпечення;

забезпечення продовольчої безпеки;

захист внутрішнього ринку від недоброякісного імпорту – поставок продукції, яка може завдавати шкоди національним виробникам, здоров'ю людей та навколишньому природному середовищу;

посилення участі України у міжнародному поділі праці, розвиток експортного потенціалу високотехнологічної продукції, поглиблення

інтеграції у європейську і світову економічну систему та активізація участі в міжнародних економічних і фінансових організаціях.

Стаття 9. **Повноваження суб'єктів забезпечення національної безпеки**

Відповідно до Конституції і законів України:

Президент України як глава держави, гарант державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина, Верховний Головнокомандувач Збройних Сил України і Голова Ради національної безпеки і оборони України здійснює загальне керівництво у сферах національної безпеки та оборони України;

Верховна Рада України в межах повноважень, визначених Конституцією України, визначає засади внутрішньої та зовнішньої політики, основи національної безпеки, формує законодавчу базу в цій сфері, схвалює рішення з питань введення надзвичайного і воєнного стану, мобілізації, визначення загальної структури, чисельності, функцій Збройних Сил України та інших військових формувань, створених відповідно до законів України;

Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сферах національної безпеки і оборони; з урахуванням змін у геополітичній обстановці вносить Президенту України пропозиції щодо уточнення Стратегії національної безпеки України та Воєнної доктрини України;

Кабінет Міністрів України як вищий орган у системі органів виконавчої влади забезпечує державний суверенітет і економічну самостійність України, вживає заходів щодо забезпечення прав і свобод людини і громадянина, обороноздатності, національної безпеки України, громадського порядку і боротьби із злочинністю;

Національний банк України відповідно до основних засад грошово-кредитної політики визначає та проводить грошово-кредитну політику в інтересах національної безпеки України;

міністерства, Служба безпеки України та інші центральні органи виконавчої влади в межах своїх повноважень забезпечують виконання передбачених Конституцією і законами України, актами Президента України, Кабінету Міністрів України завдань, здійснюють реалізацію концепцій, програм у сфері національної безпеки, підтримують у стані готовності до застосування сили та засоби забезпечення національної безпеки;

місцеві державні адміністрації та органи місцевого самоврядування забезпечують вирішення питань у сфері національної безпеки, віднесених законодавством до їхньої компетенції;

Воєнна організація держави забезпечує оборону України, захист її суверенітету, територіальної цілісності і недоторканності кордонів; протидіє зовнішнім загрозам воєнного характеру;

правоохоронні органи ведуть боротьбу із злочинністю і протидіють тероризму, забезпечують захист і врятування населення в разі виникнення надзвичайних ситуацій техногенного і природного характерів;

суди загальної юрисдикції здійснюють судочинство у справах про злочини, що завдають шкоди національній безпеці України;

прокуратура України здійснює повноваження у сфері національної безпеки України відповідно до Конституції України та Закону України «Про прокуратуру України»;

громадяни України через участь у виборах, референдумах та через інші форми безпосередньої демократії, а також через органи державної влади та органи місцевого самоврядування, які вони обирають, реалізують національні інтереси, добровільно і в порядку виконання конституційних обов'язків здійснюють заходи, визначені законодавством України щодо забезпечення її національної безпеки; як безпосередньо, так і через об'єднання громадян привертають увагу суспільних і державних інститутів до небезпечних явищ і процесів у різних сферах життєдіяльності країни; у законний спосіб і законними засобами захищають власні права та інтереси, а також власну безпеку.

Президент України Л. КУЧМА
м. Київ, 19 червня 2003 року № 964-IV

ЗАКОН УКРАЇНИ
«Про оперативно-розшукову діяльність»
ВИТЯГ

Стаття 8. Права підрозділів, які здійснюють оперативно-розшукову діяльність

Оперативним підрозділам для виконання завдань оперативно-розшукової діяльності при наявності передбачених статтею 6 цього Закону підстав надається право:

1) опитувати осіб за їх згодою, використовувати їх добровільну допомогу;

2) проводити контрольну та оперативну закупівлю та постачання товарів, предметів та речовин, у тому числі заборонених для обігу, у фізичних та юридичних осіб незалежно від форм власності з метою виявлення та документування фактів протиправних діянь. Порядок

проведення оперативної закупівлі та контрольованого постачання визначається нормативними актами Міністерства внутрішніх справ України, податкової міліції, Служби безпеки України, погодженими з Генеральною прокуратурою України та зареєстрованими у Міністерстві юстиції України;

3) порушувати в установленому законом порядку питання про проведення перевірок фінансово-господарської діяльності підприємств, установ, організацій незалежно від форм власності та осіб, які займаються підприємницькою діяльністю або іншими видами господарської діяльності індивідуально, та брати участь в їх проведенні;

4) витребувати, збирати і вивчати документи та дані, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, джерело та розміри їх доходів;

5) проводити операції по захопленню злочинців, припиненню злочинів, розвідувально-підривної діяльності спецслужб іноземних держав, організацій та окремих осіб;

6) відвідувати жилі та інші приміщення за згодою їх власників або мешканців для з'ясування обставин вчиненого або такого, що готується, злочину, а також збирати відомості про протиправну діяльність підозрюваних або осіб, щодо яких провадиться перевірка;

7) негласно виявляти та фіксувати сліди тяжкого та особливо тяжкого злочину, документи та інші предмети, що можуть бути доказами підготовки або вчинення такого злочину, чи одержувати розвідувальну інформацію, у тому числі шляхом проникнення оперативного працівника в приміщення, транспортні засоби, на земельні ділянки;

8) здійснювати проникнення в злочинну групу негласного працівника оперативного підрозділу або особи, яка співробітничає з останнім, із збереженням в таємниці достовірних даних щодо їх особистості.

Про необхідність такого проникнення виноситься постанова, яка затверджується начальником відповідного органу;

9) знімати інформацію з каналів зв'язку, застосовувати інші технічні засоби отримання інформації;

10) контролювати шляхом відбору за окремими ознаками телеграфно-поштові відправлення;

11) здійснювати візуальне спостереження в громадських місцях із застосуванням фото-, кіно- і відеозйомки, оптичних та радіоприладів, інших технічних засобів;

12) мати гласних і негласних штатних та позаштатних працівників;

13) встановлювати конфіденційне співробітництво з особами на засадах добровільності;

14) отримувати від юридичних та фізичних осіб безкоштовно або за винагороду інформацію про злочини, які готуються або вчинені, та загрозу безпеці суспільства і держави;

15) використовувати за згодою адміністрації службові приміщення, транспортні засоби та інше майно підприємств, установ, організацій, а так само за згодою осіб – житло, інші приміщення, транспортні засоби і майно, які їм належать;

16) створювати з метою конспірації підприємства, організації, використовувати документи, які зашифровують особу чи відомчу належність працівників, приміщень і транспортних засобів оперативних підрозділів;

17) створювати і застосовувати автоматизовані інформаційні системи;

18) застосовувати засоби фізичного впливу, спеціальні засоби та вогнепальну зброю на підставах і в порядку, встановлених законами про міліцію, Службу безпеки, Державну прикордонну службу України, державну охорону органів державної влади України та посадових осіб.

Негласне проникнення до житла чи до іншого володіння особи, зняття інформації з каналів зв'язку, контроль за листуванням, телефонними розмовами, телеграфною та іншою кореспонденцією, застосування інших технічних засобів одержання інформації проводяться за рішенням суду, прийнятим за поданням керівника відповідного оперативного підрозділу або його заступника. Про отримання такого дозволу суду або про відмову в ньому зазначені особи повідомляють прокурору протягом доби. Застосування цих заходів проводиться виключно з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншим способом одержати інформацію неможливо. За результатами здійснення зазначених оперативно-розшукових заходів складається протокол з відповідними додатками, який підлягає використанню як джерело доказів у кримінальному судочинстві.

Виключно з метою отримання розвідувальної інформації для забезпечення зовнішньої безпеки України, запобігання і припинення терористичних актів, розвідувально-підривних посягань спеціальних служб іноземних держав та іноземних організацій зазначені заходи можуть здійснюватись в порядку, узгодженому з Генеральним прокурором України та Головою Верховного Суду України.

Для виконання окремих доручень в ході проведення оперативно-розшукової діяльності можуть залучатись працівники інших підрозділів.

При виконанні завдань оперативно-розшукової діяльності, пов'язаних з припиненням правопорушень у сфері податкового законодавства, права,

передбачені цією статтею, надаються виключно органам податкової міліції у межах їх компетенції.

Координацію дій щодо реалізації прав підрозділів, які проводять оперативно-розшукову діяльність з метою боротьби з тероризмом, здійснює Служба безпеки України.

Президент України Л. КРАВЧУК
м. Київ, 18 лютого 1992 року
№ 2135-XII

ЗАКОН УКРАЇНИ
«Про контррозвідувальну діяльність»
ВИТЯГ

Стаття 1. **Поняття контррозвідувальної діяльності**

Контррозвідувальна діяльність – спеціальний вид діяльності у сфері забезпечення державної безпеки, яка здійснюється з використанням системи розвідувальних, контррозвідувальних, пошукових, режимних, адміністративно-правових заходів, спрямованих на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, розвідувальним, терористичним та іншим протиправним посяганням спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на інтереси України.

Стаття 2. **Мета і завдання контррозвідувальної діяльності**

Метою контррозвідувальної діяльності є попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення.

Завданнями контррозвідувальної діяльності є:

добування, аналітична обробка та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України;

протидія розвідувальній, терористичній та іншій діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України;

розроблення і реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян.

Стаття 5. **Право на здійснення контррозвідувальної діяльності**

Спеціально уповноваженим органом державної влади у сфері контррозвідувальної діяльності є Служба безпеки України.

Окремі контррозвідувальні заходи виключно в інтересах забезпечення охорони державного кордону України, посадових осіб, стосовно яких здійснюється державна охорона, а також забезпечення безпеки своїх сил і засобів, інформаційних систем та оперативних обліків можуть проводити розвідувальні органи України та Управління державної охорони України, яким законами України «Про оперативно-розшукову діяльність» та «Про розвідувальні органи України» надано право здійснювати оперативно-розшукову чи розвідувальну діяльність.

Правоохоронні та інші органи державної влади, органи місцевого самоврядування, підприємства, установи та організації України, незалежно від форми власності, в межах, визначених законами України та іншими нормативно-правовими актами, сприяють органам і підрозділам Служби безпеки України у проведенні контррозвідувальної діяльності в інтересах забезпечення державної безпеки.

Здійснення контррозвідувальних заходів іншими суб'єктами, крім визначених цим Законом, забороняється.

Стаття 6. **Підстави для проведення контррозвідувальної діяльності**

Підставами для проведення контррозвідувальної діяльності є:

1) наявність достатньої інформації, що потребує перевірки за допомогою спеціальних форм, методів і засобів, про:

здійснення розвідувальної діяльності проти України спеціальними службами іноземних держав, а також організаціями, окремими групами і особами;

посягання на державний суверенітет, конституційний лад і територіальну цілісність України;

терористичні посягання чи терористичну діяльність, злочини проти миру, безпеки людства та міжнародного правопорядку;

2) виконання визначених законом завдань щодо:

контррозвідувального забезпечення економічного, інформаційного, науково-технічного потенціалу, оборонно-промислового і транспортного комплексів та їх об'єктів, національної системи зв'язку, Збройних Сил України та інших утворених відповідно до законів України військових формувань, військово-технічного співробітництва, дотримання міжнародних режимів нерозповсюдження, а також закордонних дипломатичних установ України і безпеки громадян України за кордоном;

контррозвідувального захисту органів державної влади, правоохоронних і розвідувальних органів, охорони державної таємниці;

захисту посольств і представництв іноземних держав в Україні та їх співробітників від терористичних посягань;

вивчення і перевірки осіб, які оформлюються для допуску до державної таємниці, до роботи з ядерними матеріалами та на ядерних установках чи залучених до конфіденційного співробітництва;

забезпечення власної безпеки, у тому числі співробітників органів та підрозділів, що здійснюють контррозвідувальну діяльність, членів їх сімей та осіб, які допомагають і сприяють у здійсненні контррозвідувальної діяльності;

інформаційно-аналітичного забезпечення органів державної влади (щодо загроз державній безпеці України);

3) потреба виявлення технічними засобами і припинення роботи радіоелектронних та інших пристроїв, функціонування яких створює загрози державній безпеці України чи передумови до витоку інформації з обмеженим доступом, а також радіовипромінювань радіоелектронних засобів, що використовуються у протиправних цілях.

Президент України Л. КУЧМА
м. Київ, 26 грудня 2002 року № 374-IV

ЗАКОН УКРАЇНИ
«Про Службу безпеки України»
ВИТЯГ

Стаття 1. **Служба безпеки України**

Служба безпеки України – державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України.

Служба безпеки України підпорядкована Президенту України і підконтрольна Верховній Раді України.

Стаття 2. **Завдання Служби безпеки України**

На Службу безпеки України покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб.

До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

Стаття 24. **Обов'язки Служби безпеки України**

Служба безпеки України відповідно до своїх основних завдань зобов'язана:

1) здійснювати інформаційно-аналітичну роботу в інтересах ефективного проведення органами державної влади та управління України внутрішньої і зовнішньої діяльності, вирішення проблем оборони, соціально-економічного будівництва, науково-технічного прогресу, екології та інших питань, пов'язаних з національною безпекою України;

1) здійснює розвідувальну діяльність відповідно до закону;

2) здійснювати заходи контррозвідувального забезпечення дипломатичних представництв, консульських та інших державних установ, а також заходи, пов'язані з охороною державних інтересів у сфері зовнішньополітичної та зовнішньоекономічної діяльності, безпекою громадян України за кордоном;

3) виявляти, припиняти та розкривати злочини, розслідування яких віднесено законодавством до компетенції Служби безпеки України; проводити дізнання і слідство у цих справах; розшукувати осіб, які переховуються у зв'язку із вчиненням зазначених злочинів;

4) здійснювати контррозвідувальні заходи з метою попередження, виявлення, припинення і розкриття будь-яких форм розвідувально-підривної діяльності проти України;

5) забезпечувати захист державного суверенітету, конституційного ладу і територіальної цілісності України від протиправних посягань з боку окремих осіб та їх об'єднань;

6) здійснювати контррозвідувальне забезпечення оборонного комплексу, Збройних Сил України, інших військових формувань, дислокованих на території України, енергетики, транспорту, зв'язку, а також важливих об'єктів інших галузей господарства;

7) брати участь у розробці і здійсненні заходів щодо захисту державних таємниць України, сприяти у порядку, передбаченому законодавством, підприємствам, установам, організаціям та підприємцям у збереженні комерційної таємниці, розголошення якої може завдати шкоди життєво важливим інтересам України;

8) здійснювати відповідно до законодавства профілактику правопорушень у сфері державної безпеки;

9) у межах визначеної законодавством компетенції забезпечувати захист особистої безпеки громадян і осіб, які беруть участь у кримінальному судочинстві, у разі надходження від них, членів їх сімей та близьких родичів заяви, звернення керівника відповідного державного органу чи отримання оперативної та іншої інформації про наявність загрози їх життю, здоров'ю, житлу чи майну; брати участь у реабілітації і поновленні прав незаконно репресованих осіб;

10) сприяти Державній прикордонній службі України в охороні державного кордону України;

11) сприяти забезпеченню режиму воєнного та надзвичайного стану в разі їх оголошення, а також ліквідації наслідків стихійного лиха, значних аварій, катастроф, епідемій, епізоотій та інших надзвичайних ситуацій;

12) подавати наявними силами і засобами, в тому числі і технічними, допомогу органам внутрішніх справ, іншим правоохоронним органам у боротьбі із злочинністю;

13) брати участь у розробці заходів і вирішенні питань, що стосуються в'їзду в Україну та виїзду за кордон, перебування на її території іноземців та осіб без громадянства, прикордонного режиму і митних правил;

14) забезпечувати засекреченим і шифрованим зв'язком державні органи України і посадових осіб відповідно до переліку, який встановлюється Кабінетом Міністрів України;

15) проводити наукові дослідження і дослідно-конструкторські роботи, впроваджувати їх результати в практику діяльності Служби безпеки України;

16) виконувати за дорученням Верховної Ради України або Президента України інші завдання, безпосередньо спрямовані на забезпечення внутрішньої та зовнішньої безпеки держави;

17) брати участь у розробленні та здійсненні заходів щодо фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання, а також у проведенні спеціальної перевірки щодо допуску до особливих робіт.

Стаття 25. **Права Служби безпеки України**

Службі безпеки України, її органам і співробітникам для виконання покладених на них обов'язків надається право:

1) вимагати від громадян та посадових осіб припинення правопорушень і дій, що перешкоджають здійсненню повноважень Служби безпеки України, перевіряти у зв'язку з цим документи, які посвідчують їх особу, а також проводити огляд осіб, їх речей і транспортних засобів, якщо є загроза втечі підозрюваного або знищення чи приховання речових доказів злочинної діяльності;

2) подавати органам державного управління обов'язкові для розгляду пропозиції з питань національної безпеки України, в тому числі про припинення роботи, пов'язаної з державними таємницями, яка виконується з порушенням встановлених правил;

3) одержувати на письмовий запит керівника відповідного органу Служби безпеки України від міністерств, державних комітетів, інших відомств, підприємств, установ, організацій, військових частин, громадян

та їх об'єднань дані і відомості, необхідні для забезпечення державної безпеки України, а також користуватись з цією метою службовою документацією і звітністю. Отримання від банків інформації, яка містить банківську таємницю, здійснюється у порядку та обсязі, встановлених Законом України «Про банки і банківську діяльність»;

4) входити у порядку, погодженому з адміністрацією підприємств, установ та організацій і командуванням військових частин, на їх територію і в службові приміщення;

(Пункт 5 статті 25 виключено на підставі Закону N 488-IV від 06.02.2003)

6) використовувати з наступним відшкодуванням витрат та збитків транспортні засоби, які належать підприємствам, установам і організаціям, військовим частинам і громадянам (крім транспортних засобів дипломатичних, консульських та інших представництв іноземних держав і організацій, транспортних засобів спеціального призначення), для проїзду до місця події, припинення злочинів, переслідування та затримання осіб, які підозрюються в їх вчиненні, доставки до лікувальних установ осіб, що потребують термінової медичної допомоги;

7) виключно при безпосередньому припиненні злочинів, розслідування яких віднесено законодавством до компетенції Служби безпеки України, переслідуванні осіб, що підозрюються у їх вчиненні, заходити в жилі, службові, виробничі та інші приміщення, на території і земельні ділянки та оглядати їх з наступним повідомленням прокурора протягом 24 годин;

8) проводити гласні і негласні оперативні заходи у порядку, визначеному Законом України «Про оперативно-розшукову діяльність»;

9) здійснювати співробітництво з громадянами України та іншими особами, в тому числі на договірних засадах, дотримуючись при цьому умов добровільності і конфіденційності цих відносин;

10) користуватися на договірних засадах службовими приміщеннями підприємств, установ, організацій, військових частин, а також жилими та іншими приміщеннями громадян;

11) направляти військовослужбовців Служби безпеки України для роботи на штатних посадах в інших установах, підприємствах і організаціях на час виконання конкретних завдань в інтересах розвідки, контррозвідки, боротьби з корупцією та організованою злочинною діяльністю; в окремих випадках у порядку, визначеному колегією Служби безпеки України, допускається направлення на роботу таких військовослужбовців в установи, підприємства і організації за ініціативою їх керівників;

12) в інтересах розвідки, контррозвідки і оперативно-розшукової діяльності створювати інформаційні системи та вести оперативний облік в обсязі і порядку, що визначаються завданнями, покладеними на Службу безпеки України цим Законом;

13) морально і матеріально заохочувати співробітників Служби безпеки України та інших осіб за заслуги по забезпеченню державної безпеки; представляти їх у встановленому порядку до державних нагород;

14) позачергово придбавати квитки на всі види транспорту незалежно від наявності місць і поселятися в готелях при пред'явленні посвідчення про відрядження;

15) безплатного проїзду всіма видами міського пасажирського транспорту загального користування (крім таксі), залізничного та водного транспорту приміського сполучення та автобусами приміських маршрутів, а також попутним транспортом;

16) видавати у разі наявності небезпеки для життя і здоров'я особам, взятим під захист, відповідно до чинного законодавства зброю, спеціальні засоби індивідуального захисту та сповіщення про небезпеку.

У разі проведення заходів щодо боротьби з тероризмом і фінансуванням терористичної діяльності Служба безпеки України, її органи і співробітники мають також право:

1) одержувати в установленому законом порядку на письмову вимогу керівника органу або оперативного підрозділу Служби безпеки України від митних, фінансових та інших установ, підприємств, організацій (незалежно від форми власності) інформацію і документи про операції, стан рахунків і руху коштів на них за конкретний проміжок часу (з розшифруванням сум, дати призначення та контрагента платежу), вклади, внутрішньо- та зовнішньоекономічні угоди, а також завірені копії документів, на підставі яких було відкрито рахунок конкретної юридичної або фізичної особи. Отримання від банків відомості, яка містить банківську таємницю, здійснюється у порядку та обсязі, встановлених Законом України «Про банки і банківську діяльність». Документи та інформація повинні бути подані негайно, а якщо це неможливо – не пізніш як протягом 10 діб;

2) залучати в установленому законодавством порядку до проведення перевірок, ревізій та експертиз кваліфікованих спеціалістів установ, організацій контрольних і фінансових органів;

3) одержувати в установленому законодавством порядку за письмовими запитами керівника органу або оперативного підрозділу Служби безпеки України інформацію з автоматизованих інформаційних і довідкових систем та банків даних, створюваних Верховним Судом України, Генеральною прокуратурою України, Національним банком України, Антимонопольним комітетом України, Фондом державного майна України, міністерствами, іншими центральними органами виконавчої влади та органами місцевого самоврядування України;

4) подавати за матеріалами оперативно-розшукової діяльності до суду заяви про скасування реєстрації і припинення діяльності суб'єктів

підприємництва, а також за наявності підстав, передбачених законом, подавати до суду позови про визнання недійсними угод у порядку, встановленому законодавством України;

5) входити за письмовим розпорядженням керівника органу або оперативного підрозділу Служби безпеки України за службовими посвідченнями на територію, у приміщення, склади та сховища підприємств, організацій і установ (крім іноземних дипломатичних представництв) незалежно від форми власності, на пункти пропуску через державний кордон та митниць, а також у виробничі приміщення громадян, які займаються підприємницькою діяльністю;

6) за постановою слідчого та з санкції відповідного прокурора по нагляду за додержанням законів під час проведення оперативно-розшукової діяльності, а у невідкладних випадках – з наступним повідомленням прокурора протягом доби в разі загрози знищення, приховування або втрати предметів чи документів, які можуть бути використані в розкритті та розслідуванні злочинної діяльності, на строк до 10 діб опечатувати архіви, каси, приміщення (за винятком жилих) чи інші сховища, брати їх під охорону, накладати арешт на грошові кошти та інші цінності фізичних та юридичних осіб, вилучати предмети і документи із складанням відповідного акта. Копії акта вручаються громадянину чи представнику підприємства, установи, організації.

Органи і підрозділи Служби безпеки України, які здійснюють боротьбу з тероризмом, мають повноваження органу дізнання.

Президент України Л. КРАВЧУК
м. Київ, 25 березня 1992 року № 2229-XII

ЗАКОН УКРАЇНИ
«Про міліцію»
ВИТЯГ

Стаття 1. **Міліція в Україні**

Міліція в Україні – державний озброєний орган виконавчої влади, який захищає життя, здоров'я, права і свободи громадян, власність, природне середовище, інтереси суспільства і держави від протиправних посягань.

Стаття 2. **Основні завдання міліції**

Основними завданнями міліції є:

забезпечення особистої безпеки громадян, захист їх прав і свобод, законних інтересів;

запобігання правопорушенням та їх припинення;

охорона і забезпечення громадського порядку;
виявлення і розкриття злочинів, розшук осіб, які їх вчинили;
забезпечення безпеки дорожнього руху;
захист власності від злочинних посягань;
виконання кримінальних покарань і адміністративних стягнень;
участь у поданні соціальної та правової допомоги громадянам, сприяння у межах своєї компетенції державним органам, підприємствам, установам і організаціям у виконанні покладених на них законом обов'язків.

Стаття 10. **Основні обов'язки міліції**

Міліція відповідно до своїх завдань зобов'язана:

1) забезпечувати безпеку громадян і громадський порядок;

2) виявляти, запобігати, припиняти та розкривати злочини, вживати з цією метою оперативно-розшукових та профілактичних заходів, передбачених чинним законодавством;

3) приймати і реєструвати заяви й повідомлення про злочини та адміністративні правопорушення, своєчасно приймати по них рішення;

4) здійснювати досудову підготовку матеріалів за протокольною формою, провадити дізнання у межах, визначених кримінально-процесуальним законодавством;

5) припиняти адміністративні правопорушення і здійснювати провадження у справах про них;

6) виявляти причини й умови, що сприяють вчиненню правопорушень, вживати в межах своєї компетенції заходів до їх усунення; брати участь у правовому вихованні населення;

7) проводити профілактичну роботу серед осіб, схильних до вчинення злочинів, здійснювати адміністративний нагляд за особами, щодо яких його встановлено, а також контроль за засудженими до кримінальних покарань, не пов'язаних з позбавленням волі;

8) виконувати в межах своєї компетенції кримінальні покарання та адміністративні стягнення;

9) розшукувати осіб, які переховуються від органів дізнання, слідства і суду, ухиляються від виконання кримінального покарання, пропали безвісти, та інших осіб у випадках, передбачених законодавством;

10) проводити криміналістичні дослідження за матеріалами оперативно-розшукової діяльності, забезпечувати у встановленому порядку участь спеціалістів криміналістичної служби у слідчих діях;

11) виконувати прийняті в установленому законом порядку і в межах своєї компетенції рішення прокурора, слідчого, суду;

12) забезпечувати в межах своєї компетенції безпеку дорожнього руху, додержання законів, правил і нормативів у цій сфері, здійснювати

реєстрацію та облік автомототранспортних засобів, приймати іспити на право керування транспортними засобами і видавати відповідні документи; запобігати забрудненню повітря, водойм транспортними засобами та сільськогосподарською технікою; здійснювати контроль за утриманням у належному технічному стані та чистоті доріг, вулиць, майданів;

13) давати відповідно до законодавства дозвіл на придбання, зберігання, носіння і перевезення зброї, боєприпасів, вибухових речовин та матеріалів, інших предметів і речовин, щодо зберігання і використання яких встановлено спеціальні правила, а також на відкриття об'єктів, де вони використовуються, контролювати додержання зазначених правил та функціонування цих об'єктів;

14) контролювати додержання громадянами та службовими особами встановлених законодавством правил паспортної системи, в'їзду, виїзду, перебування в Україні і транзитного проїзду через її територію іноземних громадян та осіб без громадянства;

15) повідомляти відповідним державним органам і громадським об'єднанням про аварії, пожежі, катастрофи, стихійне лихо та інші надзвичайні події, вживати невідкладних заходів для ліквідації їх наслідків, врятування людей і подання їм допомоги, охорони майна, що залишилось без нагляду;

16) брати участь у проведенні карантинних заходів під час епідемій та епізоотій;

17) сприяти забезпеченню відповідно до законодавства режиму воєнного або надзвичайного стану, зони надзвичайної екологічної ситуації в разі їх оголошення на всій території України або в окремій місцевості;

18) охороняти на договірних засадах майно громадян, колективне і державне майно, а також майно іноземних держав, міжнародних організацій, іноземних юридичних осіб та громадян, осіб без громадянства;

19) забезпечувати збереження знайдених, вилучених у затриманих і заарештованих осіб і зданих у міліцію документів, речей, цінностей та іншого майна, вживати заходів до повернення їх законним власникам. Міліція несе відповідальність за збереження зданих цінностей і майна;

20) охороняти, конвоювати та тримати затриманих і взятих під варту осіб;

21) у встановленому порядку виявляти і повідомляти закладам охорони здоров'я про осіб, які становлять групу ризику захворювання на СНІД, і здійснювати за поданням закладу охорони здоров'я з санкції прокурора привід цих осіб, а також інфікованих вірусом імунодефіциту людини, хворих на венеричні захворювання, хронічний алкоголізм і наркоманів, які вводять наркотичні засоби шляхом ін'єкцій, для обов'язкового обстеження і лікування;

22) здійснювати привід до відповідних державних органів або установ згідно з чинним законодавством та з санкції прокурора громадян, які ухиляються від призову на військову службу;

23) подавати у межах наданих прав допомогу народним депутатам, представникам державних органів і громадських об'єднань у здійсненні їх законної діяльності, якщо їм чиниться протидія або загрожує небезпека з боку правопорушників;

24) подавати у межах наявних можливостей невідкладну, у тому числі медичну, допомогу особам, які потерпіли від правопорушень і нещасних випадків, перебувають у безпорадному або небезпечному для життя і здоров'я стані, а також неповнолітнім, які залишились без опікування;

25) забезпечувати у порядку, встановленому законодавством України, безпеку осіб, взятих під захист, у разі надходження від них заяви, звернення керівника відповідного державного органу чи отримання оперативної та іншої інформації про загрозу їх життю, здоров'ю, житлу чи майну;

26) забезпечувати виконання загальнообов'язкових рішень місцевих Рад народних депутатів, прийнятих ними в межах своєї компетенції, з питань охорони громадського порядку і правил торгівлі у невстановлених місцях, правил утримання тварин у домашніх умовах, а також контролювати утримання в належній чистоті територій дворів і прибудинкових територій у містах та інших населених пунктах;

27) забезпечувати громадський порядок під час проведення масових заходів комерційного характеру на кошти організацій або осіб, які їх проводять;

28) забезпечувати згідно із законом підтримання порядку в суді, припинення проявів неповаги до суду, а також охорону приміщень суду, виконання функції щодо державного захисту суддів, працівників суду, забезпечення безпеки учасників судового процесу.

Працівник міліції на території України незалежно від посади, яку він займає, місцезнаходження і часу в разі звернення до нього громадян або службових осіб з заявою чи повідомленням про події, які загрожують особистій чи громадській безпеці, або у разі безпосереднього виявлення таких зобов'язаний вжити заходів до попередження і припинення правопорушень, рятування людей, подання допомоги особам, які її потребують, встановлення і затримання осіб, які вчинили правопорушення, охорони місця події і повідомити про це в найближчий підрозділ міліції.

Стаття 11. **Права міліції**

Міліції для виконання покладених на неї обов'язків надається право:

1) вимагати від громадян і службових осіб, які порушують громадський порядок, припинення правопорушень та дій, що перешкоджають

здійсненню повноважень міліції, виносити на місці усне попередження особам, які допустили малозначні адміністративні порушення, а в разі невиконання зазначених вимог застосовувати передбачені цим Законом заходи примусу;

2) перевіряти у громадян при підозрі у вчиненні правопорушень документи, що посвідчують їх особу, а також інші документи, необхідні для з'ясування питання щодо додержання правил, нагляд і контроль за виконанням яких покладено на міліцію;

3) викликати громадян і службових осіб у справах про злочини та у зв'язку з матеріалами, що знаходяться в її провадженні, в разі ухилення без поважних причин від явки за викликом піддавати їх приводу у встановленому законом порядку;

4) виявляти і вести облік осіб, які підлягають профілактичному впливу на підставі та в порядку, встановлених законодавством, виносити їм офіційне застереження про неприпустимість протиправної поведінки;

5) затримувати і тримати у спеціально відведених для цього приміщеннях:

осіб, підозрюваних у вчиненні злочину, обвинувачених, які переховуються від дізнання, слідства чи суду, засуджених, які ухиляються від виконання кримінального покарання, – на строки і в порядку, передбачені законом;

осіб, щодо яких як запобіжний захід обрано взяття під варту, – на строк, встановлений органом попереднього розслідування, прокурором, судом, але не більше десяти діб;

осіб, які вчинили адміністративні правопорушення, для складання протоколу або розгляду справи по суті, якщо ці питання не можуть бути вирішені на місці, – на строк до трьох годин, а у необхідних випадках для встановлення особи і з'ясування обставин правопорушення – до трьох діб з повідомленням про це письмово прокуророві протягом 24 годин з моменту затримання;

неповнолітніх віком до 16 років, які залишилися без опікування, – на строк до передачі законним представникам або до влаштування у встановленому порядку, а неповнолітніх, які вчинили суспільно небезпечні діяння і не досягли віку, з якого настає кримінальна відповідальність, – до передачі їх законним представникам або направлення у приймальники-розподільники, але не більш як на 8 годин;

осіб, які виявили непокору законній вимозі працівника міліції, – до розгляду справи суддею;

осіб, які перебували в громадських місцях у стані сп'яніння, якщо їх вигляд ображав людську гідність і громадську мораль або якщо вони втратили здатність самостійно пересуватися чи могли завдати шкоди

оточуючим або собі, – до передачі їх в спеціальні медичні заклади або для доставки до місця проживання, а при відсутності таких – до їх витвереження;

осіб, яких запідозрено у занятті бродяжництвом, – на строк до 30 діб з санкції прокурора;

осіб, які ухиляються від виконання постанови суду про направлення на примусове лікування від хронічного алкоголізму або наркоманії, – на строк до 3 діб;

військовослужбовців, які вчинили діяння, що підпадають під ознаки злочину або адміністративного правопорушення, – до передачі їх військовослужбовцям Військової служби правопорядку у Збройних Силах України або військового командування;

осіб, які мають ознаки вираженого психічного розладу і створюють у зв'язку з цим реальну небезпеку для себе і оточуючих, – до передачі їх у лікувальні заклади, але не більш як на 24 години;

6) проводити огляд осіб, зазначених у пункті 5 цієї статті, речей, що знаходяться при них, транспортних засобів і вилучати документи та предмети, що можуть бути речовими доказами або використані на шкоду їх здоров'ю;

7) складати протоколи про адміністративні правопорушення, провадити особистий огляд, огляд речей, вилучення речей і документів, застосовувати інші передбачені законом заходи забезпечення провадження у справах про адміністративні правопорушення;

8) у випадках, передбачених Кодексом України про адміністративні правопорушення, накладати адміністративні стягнення або передавати матеріали про адміністративні правопорушення на розгляд інших державних органів, товариських судів, громадських об'єднань або трудових колективів;

9) проводити в порядку провадження дізнання і за дорученням слідчих органів у кримінальних справах обшуки, вилучення, допити та інші слідчі дії відповідно до кримінально-процесуального законодавства;

10) здійснювати на підставах і в порядку, встановлених законом, гласні та негласні оперативно-розшукові заходи, фото-, кіно-, відеозйомку і звукозапис, прослухування телефонних розмов з метою розкриття злочинів;

11) проводити фотографування, звукозапис, кіно- і відеозйомку, дактилоскопію осіб, які затримані за підозрою у вчиненні злочину або за бродяжництво, взяті під варту, звинувачуються у вчиненні злочину, а також осіб, підданих адміністративному арешту;

12) проводити кіно-, фото- і звукофіксацію як допоміжний засіб попередження протиправних дій та розкриття правопорушень;

13) вести профілактичний облік правопорушників, криміналістичний та оперативний облік в обсязі, структурі й порядку, що визначаються завданнями, покладеними на міліцію цим Законом;

14) проводити огляд поклажі, багажу та огляд пасажирів цивільних повітряних, морських і річкових суден, засобів залізничного та автомобільного транспорту згідно з чинним законодавством;

15) входити безперешкодно у будь-який час доби:

а) на територію і в приміщення підприємств, установ і організацій, в тому числі митниці, та оглядати їх з метою припинення злочинів, переслідування осіб, підозрюваних у вчиненні злочину, при стихійному лихові та інших надзвичайних обставинах;

б) на земельні ділянки, в жилі та інші приміщення громадян у разі переслідування злочинця або припинення злочину, що загрожує життю мешканців, а також при стихійному лихові та інших надзвичайних обставинах;

в) до житла чи до іншого володіння особи, яка перебуває під адміністративним наглядом, з метою перевірки виконання встановлених судом обмежень.

У разі опору, вчинення протидії працівник міліції може вжити заходів до їх подолання, передбачених цим Законом;

16) перебувати на земельних ділянках, в жилих та інших приміщеннях громадян за їхньою згодою, а також на території і в приміщеннях підприємств, установ і організацій з повідомленням про це адміністрації з метою забезпечення безпеки громадян, громадської безпеки, запобігання злочину, виявлення і затримання осіб, які його вчинили;

17) одержувати безперешкодно і безплатно від підприємств, установ і організацій незалежно від форм власності та об'єднань громадян на письмовий запит відомості (в тому числі й ті, що становлять комерційну та банківську таємницю), необхідні у справах про злочини, що знаходяться у провадженні міліції. Отримання від банків інформації, яка містить банківську таємницю, здійснюється у порядку та обсязі, встановлених Законом України «Про банки і банківську діяльність»;

18) повідомляти з метою профілактичного впливу державним органам, громадським об'єднанням, трудовим колективам і громадськості за місцем проживання особи про факти вчинення нею адміністративного правопорушення;

19) вносити відповідним державним органам, громадським об'єднанням або службовим особам, підприємствам, установам, організаціям обов'язкові до розгляду подання про необхідність усунення причин і умов, що сприяють вчиненню правопорушень;

20) відповідно до своєї компетенції тимчасово обмежувати або забороняти доступ громадян на окремі ділянки місцевості чи об'єкти з

метою забезпечення громадського порядку, громадської безпеки, охорони життя і здоров'я людей;

21) обмежувати або забороняти у випадках затримання злочинців, при аваріях, інших надзвичайних обставинах, що загрожують життю і здоров'ю людей, рух транспорту і пішоходів на окремих ділянках вулиць і автомобільних шляхів; зупиняти транспортні засоби в разі порушення правил дорожнього руху, наявних ознак, що свідчать про технічну несправність транспорту або забруднення ним навколишнього середовища, а також при наявності даних про те, що він використовується з протиправною метою; оглядати транспортні засоби і перевіряти у водіїв документи на право користування й керування ними, дорожні листи і відповідність вантажів, що перевозяться, товарно-транспортним документам; проводити технічний огляд автомототранспорту;

організовувати при необхідності медичний огляд водіїв, затримувати, відстороняти від керування транспортними засобами осіб, які перебувають у стані сп'яніння, а також тих, які не мають документів на право керування або користування транспортними засобами, позбавляти водіїв у передбачених законодавством випадках права керування транспортними засобами;

використовувати передбачені нормативними актами технічні засоби для виявлення та фіксації порушень правил дорожнього руху, забороняти експлуатацію транспортних засобів, технічний стан яких загрожує безпеці дорожнього руху чи навколишнього середовища або номери агрегатів яких не відповідають записам у реєстраційних документах; затримувати і доставляти у встановленому порядку транспортні засоби для тимчасового зберігання на спеціальних майданчиках чи стоянках;

відвідувати підприємства, установи й організації для виконання контрольних і профілактичних функцій щодо забезпечення безпеки дорожнього руху;

вимагати від відповідних організацій усунення порушень правил утримання шляхів, обмежувати або забороняти проведення ремонтно-будівельних та інших робіт, інших заходів на вулицях і автомобільних шляхах, якщо при цьому не додержуються вимоги по забезпеченню громадської безпеки;

22) анулювати виданий підприємству, установі й організації дозвіл на придбання, зберігання і використання зброї, боєприпасів, вибухових речовин і матеріалів, інших предметів і речовин при невиконанні встановлених правил користування і поводження з ними або при недоцільності їх дальшого зберігання, вилучати при необхідності зазначені предмети, опечатувати склади, бази й сховища, закривати стрілецькі тири і стенди, зброєремонтні та піротехнічні підприємства, магазини, що

торгують зброєю і боєприпасами, до усунення порушень відповідних правил;

анулювати дозволи на придбання, зберігання і носіння зброї та боєприпасів, видані громадянам, які зловживають спиртними напоями, вживають наркотичні засоби без призначення лікаря, інші одурманюючі засоби, хворіють на психічні захворювання, та в інших випадках, передбачених законодавством;

оглядати з участю адміністрації підприємств, установ, організацій приміщення, де знаходяться зброя, боєприпаси, вибухові, наркотичні та сильнодіючі хімічні, отруйні та радіоактивні речовини і матеріали, з метою перевірки додержання правил поводження з ними;

оглядати зброю та боєприпаси, що знаходяться у громадян, а також місця їх зберігання;

23) вилучати у громадян і службових осіб предмети і речі, заборонені або обмежені в обороті, а також документи з ознаками підробки, знищувати ці предмети, речі та документи або передавати їх за призначенням у встановленому порядку;

24) проводити з участю адміністрації підприємств, установ і організацій огляд виробничих, складських та інших службових приміщень і територій з метою перевірки охорони державного і колективного майна, додержання правил продажу товарів і надання послуг населенню;

вимагати від матеріально відповідальних і службових осіб підприємств, установ і організацій відомості та пояснення по фактах порушення законодавства, проведення документальних і натуральних перевірок, інвентаризацій і ревізій виробничої та фінансово-господарської діяльності; витребувати і при необхідності вилучати документи, зразки сировини й продукції, опечатувати каси, приміщення і місця зберігання документів, грошей та товарно-матеріальних цінностей;

25) користуватися безплатно всіма видами громадського транспорту міського, приміського і місцевого сполучення (крім таксі), а також попутним транспортом. Працівники підрозділів міліції на транспорті у межах обслуговуваних дільниць, крім цього, мають право на безплатний проїзд у поїздах, на річкових і морських суднах. Під час службових відряджень працівники міліції мають право на позачергове придбання квитків на всі види транспорту і розміщення в готелях при пред'явленні службового посвідчення і посвідчення про відрядження. В разі невідкладних службових поїздок вони забезпечуються квитками на проїзд незалежно від наявності місць;

26) використовувати безперешкодно транспортні засоби, що належать підприємствам, установам, організаціям і громадянам (крім транспортних засобів дипломатичних, консульських та інших представництв іноземних держав, міжнародних організацій, транспортних засобів спеціального

призначення), для проїзду до місця події, стихійного лиха, доставки в лікувальні заклади осіб, які потребують невідкладної медичної допомоги, для переслідування правопорушників та їх доставки в міліцію.

Використання з цією метою транспортних засобів, що належать підприємствам, установам і організаціям, здійснюється безплатно. Відшкодування збитків та витрат за використання транспорту громадян здійснюється відповідно до вимог статті 25 цього Закону та інших актів чинного законодавства;

27) користуватися у невідкладних випадках безперешкодно і безплатно засобами зв'язку, що належать підприємствам, установам і організаціям, а засобами зв'язку, що належать громадянам, – за їх згодою.

28) користуватися безплатно засобами масової інформації з метою встановлення обставин вчинення злочинів та осіб, які їх вчинили, свідків, потерпілих, розшуку злочинців, які втекли, осіб, які пропали безвісти, та з іншою метою, що пов'язана з необхідністю подання допомоги громадянам, підприємствам, установам і організаціям у зв'язку з виконанням міліцією покладених на неї обов'язків.

Службові особи, які без поважних причин відмовились подати допомогу працівникові міліції в реалізації його прав, передбачених пунктами 24-28 статті 11, підлягають відповідальності за чинним законодавством;

29) матеріально і морально заохочувати громадян, які подають допомогу в охороні правопорядку та боротьбі із злочинністю;

30) зберігати, носити і застосовувати спеціальні засоби та зброю;

31) видавати у разі наявності небезпеки для життя і здоров'я особам, взятим під захист, відповідно до чинного законодавства зброю, спеціальні засоби індивідуального захисту та сповіщення про небезпеку.

При здійсненні заходів із запобігання, виявлення і розкриття злочинів у сфері податкового законодавства права, передбачені цією статтею, надаються виключно органам податкової міліції у межах їх компетенції.

Голова Верховної Ради України Л. КРАВЧУК
м. Київ, 20 грудня 1990 року № 565-XII

ЗАКОН УКРАЇНИ
«Про прокуратуру»
ВИТЯГ

Стаття 1. **Прокурорський нагляд за додержанням законів в Україні**

Прокурорський нагляд за додержанням і правильним застосуванням законів Кабінетом Міністрів України, міністерствами та іншими цен-

тральними органами виконавчої влади, органами державного і господарського управління та контролю, Радою міністрів Автономної Республіки Крим, місцевими Радами, їх виконавчими органами, військовими частинами, політичними партіями, громадськими організаціями, масовими рухами, підприємствами, установами і організаціями, незалежно від форм власності, підпорядкованості та приналежності, посадовими особами та громадянами здійснюється Генеральним прокурором України і підпорядкованими йому прокурорами.

Стаття 15. **Повноваження Генерального прокурора України по керівництву органами прокуратури**

Генеральний прокурор України:

1) спрямовує роботу органів прокуратури і здійснює контроль за їх діяльністю;

2) призначає першого заступника, заступників Генерального прокурора України, керівників структурних підрозділів, головного бухгалтера, інших працівників Генеральної прокуратури України;

3) затверджує структуру і штатну чисельність підпорядкованих органів прокуратури, розподіляє кошти на їх утримання;

4) призначає за погодженням з Верховною Радою Автономної Республіки Крим прокурора Автономної Республіки Крим;

5) призначає заступників прокурора Автономної Республіки Крим, прокурорів областей, міст Києва і Севастополя, їх заступників, міських, районних, міжрайонних, а також прирівняних до них інших прокурорів;

6) відповідно до законодавства визначає порядок прийняття, переміщення та звільнення прокурорів, слідчих прокуратури та інших спеціалістів, за винятком осіб, призначення яких передбачено цим Законом;

7) відповідно до законів України видає обов'язкові для всіх органів прокуратури накази, розпорядження, затверджує положення та інструкції;

8) присвоює класні чини згідно з Положенням про класні чини працівників прокуратури. Вносить подання Президенту України про присвоєння класних чинів державного радника юстиції 1, 2 і 3 класів.

Вказівки Генерального прокурора України з питань розслідування є обов'язковими для виконання всіма органами дізнання і попереднього слідства.

Стаття 20. **Повноваження прокурора**

При здійсненні прокурорського нагляду за додержанням і застосуванням законів прокурор має право:

1) безперешкодно за посвідченням, що підтверджує займану посаду, входити у приміщення органів державної влади та органів місцевого самоврядування, об'єднань громадян, підприємств, установ та організацій незалежно від форм власності, підпорядкованості чи приналежності, до військових частин, установ без особливих перепусток, де такі запроваджено; мати доступ до документів і матеріалів, необхідних для проведення перевірки, в тому числі за письмовою вимогою, і таких, що містять комерційну таємницю або конфіденційну інформацію. Письмово вимагати подання в прокуратуру для перевірки зазначених документів та матеріалів, видачі необхідних довідок, в тому числі щодо операцій і рахунків юридичних осіб та інших організацій, для вирішення питань, пов'язаних з перевіркою. Отримання від банків інформації, яка містить банківську таємницю, здійснюється у порядку та обсязі, встановлених Законом України «Про банки і банківську діяльність»;

2) вимагати для перевірки рішення, розпорядження, інструкції, накази та інші акти і документи, одержувати інформацію про стан законності і заходи щодо її забезпечення;

3) вимагати від керівників та колегіальних органів проведення перевірок, ревізій діяльності підпорядкованих і підконтрольних підприємств, установ, організацій та інших структур незалежно від форм власності, а також виділення спеціалістів для проведення перевірок, відомчих і позавідомчих експертиз;

4) викликати посадових осіб і громадян, вимагати від них усних або письмових пояснень щодо порушень закону.

При виявленні порушень закону прокурор або його заступник у межах своєї компетенції мають право:

1) опротестовувати акти Прем'єр-міністра України, Кабінету Міністрів України, Ради міністрів Автономної Республіки Крим, міністерств та інших центральних органів виконавчої влади, виконавчих органів місцевих Рад, підприємств, установ, організацій, громадських об'єднань, а також рішення і дії посадових осіб;

2) вносити подання або протест на рішення місцевих Рад залежно від характеру порушень;

3) порушувати в установленому законом порядку кримінальну справу, дисциплінарне провадження або провадження про адміністративне правопорушення, передавати матеріали на розгляд громадських організацій;

4) давати приписи про усунення очевидних порушень закону;

5) вносити подання до державних органів, громадських організацій і посадовим особам про усунення порушень закону та умов, що їм сприяли;

6) звертатись до суду з заявою про захист прав і законних інтересів громадян, держави, а також підприємств та інших юридичних осіб.

Голова Верховної Ради України Л. КРАВЧУК
м. Київ, 5 листопада 1991 року № 1789-XII

ЗАКОН УКРАЇНИ
«Про державну податкову службу в Україні»
ВИТЯГ

Стаття 1. **Система органів державної податкової служби**

До системи органів державної податкової служби належать: Державна податкова адміністрація України, державні податкові адміністрації в Автономній Республіці Крим, областях, містах Києві та Севастополі, державні податкові інспекції в районах, містах (крім міст Києва та Севастополя), районах у містах (далі – органи державної податкової служби).

У складі органів державної податкової служби знаходяться відповідні спеціальні підрозділи по боротьбі з податковими правопорушеннями (далі – податкова міліція).

Державна податкова адміністрація України залежно від кількості платників податків та інших місцевих умов може утворювати міжрайонні (на два і більше районів), об'єднані (на місто і район) державні податкові інспекції та у їх складі відповідні підрозділи податкової міліції.

У Державній податковій адміністрації України та державних податкових адміністраціях в Автономній Республіці Крим, областях, містах Києві та Севастополі утворюються колегії. Чисельність і склад колегії Державної податкової адміністрації України затверджуються Кабінетом Міністрів України, а колегій державних податкових адміністрацій в Автономній Республіці Крим, областях, містах Києві та Севастополі – Державною податковою адміністрацією України. Колегії є дорадчими органами і розглядають найважливіші напрями діяльності відповідних державних податкових адміністрацій.

Структура Державної податкової адміністрації України затверджується Кабінетом Міністрів України.

Стаття 2. **Завдання органів державної податкової служби**

Завданнями органів державної податкової служби є:

здійснення контролю за додержанням податкового законодавства, правильністю обчислення, повнотою і своєчасністю сплати до бюджетів, державних цільових фондів податків і зборів (обов'язкових платежів), а

також неподаткових доходів, установлених законодавством (далі – податки, інші платежі);

внесення у встановленому порядку пропозицій щодо вдосконалення податкового законодавства;

прийняття у випадках, передбачених законом, нормативно-правових актів і методичних рекомендацій з питань оподаткування;

формування та ведення Державного реєстру фізичних осіб – платників податків та інших обов'язкових платежів та Єдиного банку даних про платників податків – юридичних осіб;

роз'яснення законодавства з питань оподаткування серед платників податків;

запобігання злочинам та іншим правопорушенням, віднесеним законом до компетенції податкової міліції, їх розкриття, припинення, розслідування та провадження у справах про адміністративні правопорушення.

Стаття 11. **Права органів державної податкової служби**

Органи державної податкової служби в установленому законом порядку мають право:

1) здійснювати на підприємствах, в установах і організаціях незалежно від форм власності та у громадян, в тому числі громадян – суб'єктів підприємницької діяльності, перевірки грошових документів, бухгалтерських книг, звітів, кошторисів, декларацій, товарно-касових книг, показників електронних контрольно-касових апаратів і комп'ютерних систем, що застосовуються для розрахунків за готівку із споживачами, та інших документів незалежно від способу подання інформації (включаючи комп'ютерний), пов'язаних з обчисленням і сплатою податків, інших платежів, наявності свідоцтв про державну реєстрацію суб'єктів підприємницької діяльності, спеціальних дозволів (ліцензій, патентів тощо) на її здійснення, а також одержувати від посадових осіб і громадян у письмовій формі пояснення, довідки і відомості з питань, що виникають під час перевірок; перевіряти у посадових осіб, громадян документи, що посвідчують особу, під час проведення перевірок з питань оподаткування; викликати посадових осіб, громадян для пояснень щодо джерела отримання доходів, обчислення і сплати податків, інших платежів, а також проводити перевірки достовірності інформації, одержаної для внесення до Державного реєстру фізичних осіб – платників податків та інших обов'язкових платежів.

Періодичність таких перевірок та проведення обстежень виробничих, складських, торговельних та інших приміщень встановлюється відповідно до законодавства.

Орган державної податкової служби може запрошувати громадян, в тому числі громадян – суб'єктів підприємницької діяльності, для перевірки правильності нарахування та своєчасності сплати ними податків, інших платежів. Письмові повідомлення про такі запрошення направляються громадянам рекомендованими листами, в яких зазначаються підстави виклику, дата і година, на яку викликається громадянин;

2) одержувати безоплатно від підприємств, установ, організацій, включаючи Національний банк України та його установи, комерційні банки та інші фінансово-кредитні установи (у порядку, передбаченому законодавством для розкриття банківської таємниці), від громадян – суб'єктів підприємницької діяльності довідки, копії документів про фінансово-господарську діяльність, отримані доходи, видатки підприємств, установ і організацій незалежно від форм власності та громадян про поточні та вкладні (депозитні) рахунки, інформацію про наявність та обіг коштів на цих рахунках, у тому числі про ненадходження у встановлені терміни валютної виручки від суб'єктів підприємницької діяльності, та іншу інформацію, пов'язану з обчисленням та сплатою податків, інших платежів у порядку, визначеному законодавством, входити в будь-які інформаційні системи, зокрема комп'ютерні, для визначення об'єкта оподаткування;

одержувати безоплатно необхідні відомості для формування інформаційного фонду Державного реєстру фізичних осіб – платників податків та інших обов'язкових платежів від підприємств, установ, організацій незалежно від форм власності, включаючи Національний банк України та його установи, комерційні банки, та громадян – суб'єктів підприємницької діяльності – про суми доходів, виплачених фізичним особам, і утриманих з них податків, інших платежів, від органів, уповноважених проводити державну реєстрацію, а також видавати спеціальні дозволи (ліцензії, патенти тощо) на здійснення деяких видів підприємницької діяльності, – про видачу таких дозволів суб'єктам підприємницької діяльності, від органів внутрішніх справ – про громадян, які прибули на проживання до відповідного населеного пункту чи вибули з нього, від органів реєстрації актів громадянського стану – про громадян, які померли;

одержувати безоплатно від митних органів щомісяця звітні дані про ввезення на митну територію України імпортних товарів і справляння при цьому податків, інших платежів та інформацію про експортно-імпортні операції, що здійснюють резиденти і нерезиденти, за формою, погодженою з Державною податковою адміністрацією України, та від органів статистики – дані, необхідні для використання їх у проведенні аналізу фінансово-господарської діяльності підприємств, установ, організацій всіх форм власності;

3) обстежувати будь-які виробничі, складські, торговельні та інші приміщення підприємств, установ і організацій незалежно від форм власності та житло громадян, якщо вони використовуються як юридична адреса суб'єкта підприємницької діяльності, а також для отримання доходів. У разі відмови керівників підприємств, установ, організацій і громадян допустити посадових осіб органів державної податкової служби для обстеження зазначених приміщень і обладнання та неподання документів про отримані доходи і проведені витрати органи державної податкової служби мають право визначати оподатковуваний доход (прибуток) таких підприємств, установ, організацій та громадян на підставі документів, що свідчать про одержані ними доходи (прибутки), а стосовно громадян – також із урахуванням оподаткування осіб, які займаються аналогічною діяльністю;

4) вимагати від керівників та інших посадових осіб підприємств, установ, організацій, а також від громадян, діяльність яких перевіряється, усунення виявлених порушень податкового законодавства і законодавства про підприємницьку діяльність, контролювати їх виконання, а також припинення дій, які перешкоджають здійсненню повноважень посадовими особами органів державної податкової служби;

(Пункт 5 частини першої статті 11 виключено на підставі Закону N 2181-III від 21.12.2000 – набирає чинності з 1 квітня 2001 року)

6) вилучати (із залишенням копій) у підприємств, установ та організацій документи, що свідчать про приховування (заниження) об'єктів оподаткування, несплату податків, інших платежів, та вилучати у громадян – суб'єктів підприємницької діяльності, які порушують порядок заняття підприємницькою діяльністю, реєстраційні посвідчення або спеціальні дозволи (ліцензії, патенти тощо) з наступною передачею матеріалів про порушення органам, що видали ці документи;

7) застосовувати до підприємств, установ, організацій і громадян фінансові санкції у порядку та розмірах, встановлених законом;

застосовувати до юридичних осіб, фізичних осіб – суб'єктів підприємницької діяльності, які у встановлений законом строк не повідомили про відкриття або закриття рахунків у фінансових установах, а також до фінансових установ, що не подали відповідним органам державної податкової служби в установлений законом строк повідомлень про закриття рахунків платників податків або розпочали здійснення видаткових операцій за рахунком платника податків – суб'єкта підприємницької діяльності (крім банків) до отримання документально підтвердженого повідомлення відповідного органу державної податкової служби про взяття рахунку на облік в органах державної податкової служби, штрафні санкції у розмірі двадцяти неоподатковуваних мінімумів доходів громадян;

8) стягувати до бюджетів та державних цільових фондів суми недоїмки, пені та штрафних санкцій у порядку, передбаченому законом;

9) надавати відстрочення та розстрочення податкових зобов'язань, вирішувати питання щодо податкового компромісу, а також приймати рішення про списання безнадійного боргу у порядку, передбаченому законом;

10) за несвоєчасне виконання установами банків та іншими фінансово-кредитними установами розпоряджень органів державної податкової служби про безспірне стягнення податків, інших платежів, а також доручень підприємств, установ, організацій та громадян про сплату податків, інших платежів стягувати з установ банків та інших фінансово-кредитних установ пеню за кожний день прострочення (включаючи день сплати) у розмірах, встановлених законодавством щодо таких видів платежів;

11) накладати адміністративні штрафи:

на керівників та інших посадових осіб підприємств, установ, організацій, винних у відсутності податкового обліку або веденні його з порушенням встановленого порядку, неподанні або несвоєчасному поданні аудиторських висновків, передбачених законом, а також платіжних доручень на перерахування належних до сплати податків, зборів (обов'язкових платежів), – від п'яти до десяти неоподатковуваних мінімумів доходів громадян, а за ті самі дії, вчинені особою, яку протягом року було піддано адміністративному стягненню за відповідне правопорушення, – від десяти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян;

на керівників та інших посадових осіб підприємств, установ, організацій, включаючи установи Національного банку України, комерційні банки та інші фінансово-кредитні установи, які не виконують перелічених у пунктах 2 – 5 цієї статті вимог посадових осіб органів державної податкової служби, – від десяти до двадцяти неоподатковуваних мінімумів доходів громадян;

на посадових осіб підприємств, установ і організацій, а також на громадян – суб'єктів підприємницької діяльності, які виплачували доходи, винних у неутриманні, неперерахуванні до бюджету сум податку на доходи фізичних осіб, перерахуванні податку за рахунок коштів підприємств, установ і організацій (крім випадків, коли таке перерахування дозволено законодавством), у перекрученні даних, у неповідомленні або несвоєчасному повідомленні державним податковим інспекціям за встановленою формою відомостей про доходи громадян,- у розмірі трьох неоподатковуваних мінімумів доходів громадян, а за ті самі дії, вчинені особою, яку протягом року було піддано адміністративному стягненню за одне із зазначених правопорушень, – у розмірі п'яти неоподатковуваних мінімумів доходів громадян;

на громадян, винних у неподанні або несвоєчасному поданні декларацій про доходи чи у включенні до декларацій перекручених даних, у відсутності обліку або неналежному веденні обліку доходів і витрат, для яких встановлено обов'язкову форму обліку, – від одного до п'яти неоподатковуваних мінімумів доходів громадян;

на громадян, які займаються підприємницькою діяльністю, винних у протидіях посадовим особам органів державної податкової служби, зокрема у недопущенні їх до приміщень, які використовуються для здійснення підприємницької діяльності та одержання доходів, – від десяти до двадцяти неоподатковуваних мінімумів доходів громадян;

на громадян, які займаються підприємницькою діяльністю без державної реєстрації чи без спеціального дозволу (ліцензії), якщо його отримання передбачено законодавством, – від трьох до восьми неоподатковуваних мінімумів доходів громадян;

на громадян, які здійснюють продаж товарів без придбання одноразових патентів або з порушенням терміну їх дії, чи здійснюють продаж товарів, не зазначених у деклараціях, – від одного до десяти неоподатковуваних мінімумів доходів громадян, а за ті самі дії, вчинені громадянином, якого протягом року було піддано адміністративному стягненню за одне із зазначених правопорушень, – від десяти до двадцяти неоподатковуваних мінімумів доходів громадян;

12) користуватися безперешкодно в службових справах засобами зв'язку, які належать підприємствам, установам і організаціям незалежно від форм власності;

13) у разі виявлення зловживань під час здійснення контролю за надходженням валютної виручки, проведенням розрахунків із споживачами з використанням товарно-касових книг, а також за дотриманням лімітів готівки в касах та її використанням для розрахунків за товари, роботи і послуги давати доручення органам державної контрольно-ревізійної служби на проведення ревізій;

14) вимагати від керівників підприємств, установ і організацій, що перевіряються, проведення інвентаризації основних фондів, товарно-матеріальних цінностей, коштів і розрахунків; при проведенні адміністративного арешту опечатувати каси, касові приміщення, склади та архіви;

15) надавати інформацію з Державного реєстру фізичних осіб – платників податків та інших обов'язкових платежів іншим державним органам відповідно до чинного законодавства;

16) матеріально і морально заохочувати громадян, які подають допомогу в боротьбі з порушеннями податкового законодавства;

17) звертатися у передбачених законом випадках до суду з заявою (позовною заявою) про скасування державної реєстрації суб'єкта підприємницької діяльності.

Права, передбачені пунктами 1-4, 6, 12 і 14 частини першої цієї статті, надаються посадовим особам органів державної податкової служби, а права, передбачені пунктами 5, 7 – 11, 13, 15- 17, – головам державних податкових адміністрацій і начальникам державних податкових інспекцій та їх заступникам;

Стаття 13. **Обов'язки і відповідальність по**садових осіб органів державної податкової служби

Посадові особи органів державної податкової служби зобов'язані дотримувати Конституції і законів України, інших нормативних актів, прав та охоронюваних законом інтересів громадян, підприємств, установ, організацій, забезпечувати виконання покладених на органи державної податкової служби функцій та повною мірою використовувати надані їм права.

За невиконання або неналежне виконання посадовими особами органів державної податкової служби своїх обов'язків вони притягаються до дисциплінарної, адміністративної, кримінальної та матеріальної відповідальності згідно з чинним законодавством.

Збитки, завдані неправомірними діями посадових осіб органів державної податкової служби, підлягають відшкодуванню за рахунок коштів державного бюджету.

Посадові особи органів державної податкової служби зобов'язані дотримувати комерційної та службової таємниці.

Голова Верховної Ради Української РСР Л. КРАВЧУК
м. Київ, 4 грудня 1990 року № 509-XII

ЗАКОН УКРАЇНИ
«Про місцеве самоврядування в Україні»
ВИТЯГ

Стаття 2. Поняття місцевого самоврядування

1. Місцеве самоврядування в Україні – це гарантоване державою право та реальна здатність територіальної громади – жителів села чи добровільного об'єднання у сільську громаду жителів кількох сіл, селища, міста – самостійно або під відповідальність органів та посадових осіб місцевого самоврядування вирішувати питання місцевого значення в межах Конституції і законів України.

2. Місцеве самоврядування здійснюється територіальними громадами сіл, селищ, міст як безпосередньо, так і через сільські, селищні, міські ради та їх виконавчі органи, а також через районні та обласні ради, які представляють спільні інтереси територіальних громад сіл, селищ, міст.

Стаття 28. **Повноваження в галузі бюджету, фінансів і цін**

До відання виконавчих органів сільських, селищних, міських рад належать:

а) власні (самоврядні) повноваження:

1) складання проекту місцевого бюджету, подання його на затвердження відповідної ради, забезпечення виконання бюджету; щоквартальне подання раді письмових звітів про хід і результати виконання бюджету; підготовка і подання відповідно до районних, обласних рад необхідних фінансових показників і пропозицій щодо складання проектів районних і обласних бюджетів;

2) встановлення в порядку і межах, визначених законодавством, тарифів щодо оплати побутових, комунальних, транспортних та інших послуг, які надаються підприємствами та організаціями комунальної власності відповідної територіальної громади; погодження в установленому порядку цих питань з підприємствами, установами та організаціями, які не належать до комунальної власності;

3) встановлення за узгодженим рішенням відповідних рад порядку використання коштів та іншого майна, що перебувають у спільній власності територіальних громад;

4) здійснення в установленому порядку фінансування видатків з місцевого бюджету;

5) залучення на договірних засадах коштів підприємств, установ та організацій незалежно від форм власності, розташованих на відповідній території, та коштів населення, а також бюджетних коштів на будівництво, розширення, ремонт і утримання на пайових засадах об'єктів соціальної і виробничої інфраструктури та на заходи щодо охорони навколишнього природного середовища;

6) об'єднання на договірних засадах коштів відповідного місцевого бюджету та інших місцевих бюджетів для виконання спільних проектів або для спільного фінансування комунальних підприємств, установ та організацій, вирішення інших питань, що стосуються спільних інтересів територіальних громад;

б) делеговані повноваження:

1) здійснення відповідно до закону контролю за дотриманням зобов'язань щодо платежів до місцевого бюджету на підприємствах і в організаціях незалежно від форм власності;

2) здійснення відповідно до закону контролю за дотриманням цін і тарифів;

3) сприяння здійсненню інвестиційної діяльності на відповідній території.

Президент України Л. КУЧМА

м. Київ, 21 травня 1997 року № 280/97-ВР

Додаток В.4

УКАЗ ПРЕЗИДЕНТА УКРАЇНИ
«Про невідкладні додаткові заходи щодо посилення боротьби з організованою злочинністю і корупцією»
ВИТЯГ

4. Керівникам міністерств, інших центральних органів виконавчої влади, Голові Ради міністрів Автономної Республіки Крим, головам обласних, Київської та Севастопольської міських державних адміністрацій удосконалити та посилити взаємодію з правоохоронними органами, систематично аналізувати стан злочинності та корупції у пріоритетних галузях економіки та в регіонах, здійснювати за їх результатами скоординовані заходи щодо боротьби з такими явищами.

Особливу увагу звернути на протидію намаганням організованих злочинних угруповань контролювати підприємницьку діяльність, функціонування об'єктів паливно-енергетичного та агропромислового комплексів, фінансову та банківську сфери.

8. Кабінету Міністрів України, Міністерству внутрішніх справ України, Службі безпеки України, Державній податковій адміністрації України, Державній митній службі України, Державному комітету у справах охорони державного кордону України, іншим центральним органам виконавчої влади за участю Генеральної прокуратури України:

а) розробити та здійснити спільні заходи, спрямовані на:

суттєве посилення боротьби з корупцією та хабарництвом, приділивши особливу увагу викриттю корупційних діянь серед державних службовців та інших посадових осіб, усуненню причин і умов, що цьому сприяють;

знешкодження суспільно небезпечних організованих корисливо-насильницьких злочинних угруповань, посилення протидії незаконному обігу наркотичних засобів, зброї та вибухових речовин;

ефективну протидію злочинам у сфері економіки, передусім в її пріоритетних галузях, захист від злочинних зазіхань на державні бюджетні кошти;

викриття фактів легалізації (відмивання) доходів, одержаних злочинним шляхом;

забезпечення надійної охорони державного кордону, перекриття каналів проникнення в Україну нелегальних мігрантів, предметів

контрабанди, зокрема наркосировини, зброї, боєприпасів та інших засобів вчинення тяжких та особливо тяжких злочинів;

в) зосередити зусилля на знешкодженні організованих злочинних угруповань, які використовують кримінальні доходи для приватизації об'єктів паливно-енергетичного комплексу, вугледобувної та металургійної промисловості, сфери обслуговування та інших прибуткових сфер економіки, виявляти та припиняти злочини, які вчиняються під час здійснення підприємствами, які є економічною основою злочинних угруповань, фінансово-господарських операцій в офшорних зонах;

10. Державній податковій адміністрації України, Міністерству фінансів України, Міністерству внутрішніх справ України, Службі безпеки України, Національному банку України:

перевірити законність джерел походження коштів, що залучаються для формування статутних капіталів банків та інших фінансових установ;

проаналізувати ефективність протидії легалізації (відмиванню) коштів та іншого майна, одержаних злочинним шляхом організованими злочинними угрупованнями з використанням фінансових установ та інших комерційних структур, зареєстрованих в офшорних зонах;

ужити заходів щодо закриття каналів незаконного відтоку капіталів за кордон.

12. Фонду державного майна України, Міністерству внутрішніх справ України, Службі безпеки України, Державній податковій адміністрації України за участю Генеральної прокуратури України забезпечувати жорсткий контроль за виконанням умов кожного договору купівлі-продажу стратегічно важливих об'єктів, запобігати фактам приватизації через компанії, зареєстровані в офшорних зонах, як форму приховування реальних власників, джерел походження коштів і ухилення від сплати податків.

14. Кабінету Міністрів України, Раді міністрів Автономної Республіки Крим, обласним, Київській та Севастопольській міським державним адміністраціям:

розробити програми правових, організаційних заходів щодо детінізації економіки, припинення криміналізації економічної сфери, захисту фінансової та банківської систем, паливно-енергетичного та агропромислового комплексів від злочинних посягань;

забезпечити додержання законодавства в бюджетній сфері, вжити заходів щодо протидії незаконному розподілу, розкраданню, нецільовому використанню бюджетних коштів та попередити керівників міністерств,

інших центральних і місцевих органів виконавчої влади, державних промислових підприємств про персональну відповідальність за наведення порядку у здійсненні фінансових операцій, про недопущення розрахунків бюджетними коштами шляхом взаємозаліків та дисконтними векселями;

передбачити виділення коштів для матеріально-технічного забезпечення спеціальних підрозділів по боротьбі з організованою злочинністю і корупцією, закупівлі сучасної спеціальної техніки для виявлення нових способів вчинення злочинів;

Президент України Л. КУЧМА
м. Київ, 6 лютого 2003 року № 84/2003

УКАЗ ПРЕЗИДЕНТА УКРАЇНИ
«Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень»
ВИТЯГ

2. Кабінету Міністрів України за участю Національного банку України з метою забезпечення сприятливих умов кредитування комерційними банками суб'єктів підприємницької діяльності, цільового використання одержаних кредитів та своєчасного їх повернення:

розробити та внести до 1 грудня 2000 року в установленому порядку на розгляд Верховної Ради України законопроект про кредитування, в якому передбачити вирішення питань захисту прав та інтересів кредиторів, посилення відповідальності учасників договірних відносин за неналежне виконання своїх зобов'язань;

удосконалити порядок реалізації заставленого майна з метою захисту інтересів кредиторів;

розробити фіскальні та монетарні стимули для банків, що збільшують обсяги довгострокового кредитування виробництва;

сприяти розвитку та зміцненню конкурентних позицій інвестиційних компаній, довірчих товариств, кредитних спілок, страхових компаній, брокерських контор тощо, утворити у встановленому порядку відповідний державний орган з контролю за їх діяльністю;

забезпечити стимулювання зростання обсягів грошових вкладів населення через створення умов економічної заінтересованості та розширення гарантій збереження таких вкладів;

вжити заходи щодо розвитку іпотечного кредитування;

розробити механізми стимулювання лізингу шляхом удосконалення системи оподаткування лізингових операцій, у тому числі нарахування амортизації на об'єкт лізингу;

розробити заходи, спрямовані на пожвавлення інвестиційної діяльності комерційних банків шляхом придбання цінних паперів, емітованих суб'єктами підприємницької діяльності;

посилити захист інтересів комерційних банків у процесах приватизації державного майна та реорганізації підприємств, передбачивши участь банку-кредитора у перерозподілі заборгованості за банківськими кредитами між правонаступниками приватизованого або реорганізованого підприємства;

вирішити в установленому порядку питання щодо віднесення комерційними банками на валові витрати коштів, що спрямовуються на формування резервів, створюваних для відшкодування можливих втрат за активними операціями, а також щодо спрощення процедури списання безнадійної заборгованості за рахунок резервів;

вирішити протягом 2000 року питання щодо створення за участю комерційних банків єдиної інформаційної системи обліку позичальників (боржників), які мають прострочену заборгованість за кредитами, наданими комерційними банками, із зазначенням її обсягів;

забезпечити вирішення у передбаченому законом порядку питання щодо встановлення адміністративної та кримінальної відповідальності за розголошення банківської таємниці;

розробити та реалізувати протягом 2001 - 2003 років програму перепідготовки кадрів для банків з метою підвищення рівня менеджменту банківської діяльності, використавши на ці цілі асигнування комерційних банків та міжнародну технічну допомогу;

сприяти прийняттю Верховною Радою України нової редакції Закону України «Про банки та банківську діяльність», законів про вексельний обіг, про іпотеку, про фонд гарантування вкладів фізичних осіб, про валютне регулювання, про державну реєстрацію прав на нерухоме майно (в тому числі права застави).

4. Кабінету Міністрів України опрацювати та внести на розгляд Верховної Ради України законопроекти про:

систему заходів щодо погашення знецінених грошових заощаджень громадян, яке передбачено Законом України «Про державні гарантії відновлення заощаджень громадян України», з метою визначення додаткових механізмів погашення таких заощаджень;

зміни та доповнення до Кримінального кодексу України щодо запровадження відповідальності за виготовлення, збут та використання підроблених платіжних документів і засобів несанкціонованого доступу до банківських рахунків;

зміни та доповнення до податкового законодавства, які б ураховували специфіку банківської діяльності, в тому числі щодо звільнення ко-

мерційних банків від часткової сплати податку на прибуток, який виникає від переоцінки власного капіталу банку внаслідок девальвації гривні;

встановлення з метою запобігання дискредитації банківської системи та дестабілізації діяльності банків відповідальності посадових осіб за порушення шляхом передчасного розголошення інформації (в тому числі через засоби масової інформації) вимог законодавства щодо таємниці слідства.

Президент України Л. КУЧМА
м. Київ, 14 липня 2000 року № 891/2000

Додаток В.5

КОМІТЕТ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ ФІНАНСІВ І БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

ЛИСТ № 06-10/678 від 19.11.2001

Комітет Верховної Ради України з питань фінансів та банківської діяльності розглянув запит щодо деяких аспектів розкриття банківськими установами за власною ініціативою банківської таємниці і повідомляє.

Відповідно до ст. 64 Закону України «Про банки і банківську діяльність» установи банків зобов'язані ідентифікувати клієнтів, які здійснюють значні та сумнівні операції, та за власною ініціативою без відповідного запиту надавати інформацію щодо ідентифікованих осіб спеціальним органам по боротьбі з організованою злочинністю.

Значними операціями з готівковими коштами відповідно до частини третьої ст. 64 Закону України «Про банки і банківську діяльність» є угоди з готівкою на суми, що перевищують еквівалент 10000 євро за офіційним курсом гривні до іноземної валюти, встановленим Національним банком України.

Оскільки відповідно до п. 78 Інструкції Національного банку України № 1 з організації емісійно-касової роботи в установах банків України видача готівки з кас банків відбувається на підставі грошових чеків або видаткових касових ордерів, то у випадку отримання готівкових коштів з кас банків під операцією з готівкою на суму, що перевищує еквівалент 10000 євро за офіційним курсом гривні до іноземної валюти, встановленим Національним банком України, мається на увазі отримання готівки на суму, що перевищує зазначений еквівалент, на підставі одного грошового чека або видаткового касового ордеру. А відповідно до п. 4.18 Інструкції Національного банку України про організацію роботи з готівкового обігу установами банків України цільове призначення готівки, яку одержують підприємства (підприємці) зі своїх поточних рахунків, має зазначатися ними в грошовому чеку з чітким формулюванням суті операцій, що будуть здійснюватися. Згідно з частиною п'ятою ст. 64 Закону України «Про банки і банківську діяльність» ідентифікації та відповідно наступному повідомленню щодо ідентифікованих осіб відповідних органів по боротьбі з організованою злочинністю підлягають також особи, які здійснюють

розрахунки за угодами на суму нижчу, ніж передбачено для значних операцій, якщо така угода явно пов'язана з іншою угодою і загальна сума оплати за цими угодами перевищує встановлену межу.

Отже, якщо клієнт банківської установи отримує готівкові кошти протягом одного операційного дня за різними грошовими чеками і загальна сума за такими чеками складає понад еквівалент 10000 євро, то у випадку застосування цих коштів для розрахунків за угодами, що явно не пов'язані одна з одною, тобто при розрахунках з різними контрагентами або для витрат у різних цілях, здійснення повідомлення органів по боротьбі з організованою злочинністю про осіб, ідентифікованих за такими операціями, не потрібне.

Щодо віднесення операцій з отримання готівкових коштів до сумнівних операцій, то частиною четвертою ст. 64 Закону України «Про банки і банківську діяльність» передбачено перелік ознак таких операцій, до яких відноситься:

1) здійснення операцій за незвичних або невиправдано заплутаних умов;

2) операція не є економічно виправданою або суперечить законодавству України. Даний перелік є вичерпним та не підлягає розширеному тлумаченню.

Таким чином, зняття клієнтом банку готівкових коштів зі свого рахунка, якщо така операція не містить вищевказаних ознак, є звичною для клієнта та проводиться ним постійно, відповідає характеру його діяльності тощо, не може бути кваліфіковане як сумнівне з наступним повідомленням про нього спеціальних органів по боротьбі з організованою злочинністю без наявності оформленого відповідно до вимог діючого законодавства запиту.

Голова Комітету В. Альошин
«Бухгалтерія», N 49/1, 3 грудня 2001 р.

Додаток В.6

ПОСТАНОВИ ТА ЛИСТИ ПРАВЛІННЯ НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ

Від 28 березня 2001 р. № 134

Зареєстровано в Міністерстві юстиції України
12 квітня 2001 р. за № 338/5529

Про затвердження Інструкції про вимоги
з організації охорони установ банків України

Згідно зі статтею 33 Закону України «Про Національний банк України» Правління Національного банку України

п о с т а н о в л я є:

1. Затвердити Інструкцію про вимоги з організації охорони установ банків України (далі – Інструкція), що додається (для службового користування).

2. Визнати такими, що втратили чинність, Правила залучення до охорони установ банків IV – V категорій охорони суб'єктів підприємницької діяльності, які отримали ліцензії на надання охоронних послуг, затверджені постановою Правління Національного банку України від 05.07.99 № 322 та зареєстровані в Міністерстві юстиції України 21.07.99 за № 490/3783.

Голова В.С. Стельмах

від 18 червня 2003 р. № 254
Зареєстровано в Міністерстві юстиції України 8 липня 2003 р. за № 559/7880
Про затвердження Положення про організацію операційної діяльності
в банках України

9.5. Програмне забезпечення банку має відповідати таким вимогам інформаційної безпеки:

наявність системи захисту інформації, яку не можна відключити і неможливо здійснити оброблення інформації без її використання;

забезпечення належного захисту інформації під час її передавання між різними підсистемами формування та оброблення інформації;

для автоматизованих систем, які функціонують у режимі «клієнт-сервер», доступ користувачів до бази даних має відбуватися лише через додаткове програмне забезпечення, за допомогою якого здійснюється автентифікація осіб, яким дозволено користуватися цією базою даних;

автентифікація користувача на кожному робочому місці та під час здійснення будь-яких операцій;

забезпечення блокування роботи на кожному робочому місці під час багаторазових спроб (не більше трьох) неправильного введення паролю, якщо використовується парольний захист;

наявність безперервного технологічного контролю за цілісністю інформації та накладання/перевіряння цифрового підпису на всіх банківських документах на всіх етапах їх оброблення;

передавання електронних банківських документів, втрата або несанкціоноване ознайомлення з якими може завдати збитків банку, його установі або клієнту банку, відповідними каналами зв'язку електронною поштою або в режимі о№-лі№е лише зашифрованими з обов'язковим наданням підтвердження про їх отримання;

обов'язкова реєстрація всіх спроб доступу, усіх операцій та інших дій, їх фіксація в автоматизованій системі в захищеному від модифікації електронному журналі з постійним контролем його цілісності.

Крім того, банкам слід:

суворо дотримуватися і перевіряти виконання вимог щодо технічного та технологічного забезпечення їх діяльності, зокрема розміщення програмно-апаратних комплексів на таких комп'ютерах, що мають забезпечити їх надійне функціонування;

уживати заходів для забезпечення безперебійного електроживлення та наявності резервних каналів зв'язку;

перевіряти виконання вимог щодо організації захисту інформації в програмно-технічних комплексах згідно з нормативно-правовими актами Національного банку та вимогами розробників систем захисту інформації.

Головний бухгалтер – директор Департаменту бухгалтерського обліку В.І. Ричаківська

від 8 липня 1998 р. № 267
Зареєстровано в Міністерстві юстиції України 2 вересня 1998 р. за № 546/2986

Про порядок передачі інформації від установ банків до органів державної податкової служби електронними засобами

Правління
п о с т а н о в л я є:

1. Затвердити Порядок передачі інформації від установ банків до органів державної податкової служби електронними засобами з питань проведення операцій відкриття, закриття рахунків; зарахування податків, повернення надмірно сплачених сум; реєстру розрахункових документів про сплату платежів до бюджету; щоденної банківської звітності за формою 412-Д (додається).

3. Контроль за виконанням цієї постанови покласти на члена Правління – директора Департаменту інформатизації.

В.О. Голови В.С. Стельмах

ЗАТВЕРДЖЕНО

Наказ Державної податкової адміністрації України 02.07.98 р. № 317
Постанова Правління Національного банку України 08.07.98 р. № 267
Зареєстровано в Міністерстві юстиції України 2 вересня 1998 р. за № 546/2986

Порядок передачі інформації від установ банків до органів державної податкової служби електронними засобами з питань проведення операцій відкриття, закриття рахунків; зарахування податків, повернення надмірно сплачених сум; реєстру розрахункових документів про сплату платежів до бюджету; щоденної банківської звітності за формою 412-Д

1. Національний банк України, комерційні банки та їх установи зобов'язані:

1.1. Надавати інформацію відповідно до пунктів 1.2 – 1.4 в електронному вигляді засобами електронної пошти НБУ на адресу державних податкових адміністрацій (далі – ДПА) в Автономній Республіці Крим, областях, містах Києві та Севастополі з використанням засобів захисту Національного банку України (далі – НБУ).

7. Відповідальність за зберігання та нерозголошення конфіденційної банківської інформації в обчислювальних мережах ДПА покладається на податкові органи згідно з чинним законодавством.

8. Захист інформації, яка передається електронною поштою ДПА від обласних податкових органів місцевим податковим органам, здійснюється засобами захисту ДПА України.

9. Контроль за виконанням вимог цього Порядку покласти на ДПА в Автономній Республіці Крим, областях, містах Києві і Севастополі та на регіональні управління НБУ.

№ 280 від 10.06.99 Зареєстровано в Міністерстві юстиції України
30 серпня 1999 р.
м.Київ за № 583/3876

Про затвердження Правил організації захисту електронних банківських документів

(Із змінами, внесеними згідно з Постановою Національного банку № 495 від 04.12.2001)

Правління П О С Т А Н О В Л Я Є:

1. Затвердити Правила організації захисту електронних банківських документів в установах, включених до інформаційно-обчислювальної мережі Національного банку України (додаються) та Правила організації захисту електронних банківських документів в установах Національного банку України (тільки до служб захисту установ НБУ).

2. Керівникам банківських установ, начальникам Кримського республіканського, по м. Києву і області, обласних, Операційного, Головного управлінь Національного банку України, начальнику Центральної розрахункової палати протягом місяця з дня набуття чинності цієї постанови привести у відповідність із правилами організації захисту електронних банківських документів усі заходи організації захисту в установах.

3. Ця постанова набуває чинності через десять днів після державної реєстрації в Міністерстві юстиції України.

Голова В.А. Ющенко

Правила організації захисту електронних банківських документів в установах, включених до інформаційно-обчислювальної мережі Національного банку України

1. Загальні положення

1.2. Правила регламентують порядок отримання, обліку, передачі, використання та зберігання засобів криптозахисту НБУ, виконання правил інформаційної безпеки в установах, що є учасниками інформаційно-обчислювальної мережі Національного банку України.

1.3. Положення цього документа поширюються на всі установи, що працюють в інформаційно-обчислювальній мережі НБУ та мають програмний комплекс АРМ-НБУ й засоби криптографічного захисту НБУ.

1.5. У разі виникнення ситуацій, не передбачених цим документом, їх необхідно розглядати в робочому порядку через службу захисту інформації регіонального управління та управління захисту інформації НБУ.

1.6. Відповідальність за виконання вимог захисту в середині банківської установи покладається на керівництво цієї установи.

2. Принципи побудови системи захисту...

2.3. Система захисту електронних банківських документів складається з комплексу апаратно-програмних засобів криптографічного захисту та ключової системи до них, технологічних і організаційних заходів щодо захисту інформації в інформаційно-обчислювальній мережі НБУ.

2.4. Система захисту електронних банківських документів охоплює всі етапи розробки, впровадження та експлуатації програмно-технічного забезпечення інформаційно-обчислювальної мережі та включає чіткий розподіл відповідальності на кожному етапі підготовки, обробки та виконання електронних банківських документів на всіх рівнях.

2.5. Система захисту електронних банківських документів в інформаційно-обчислювальній мережі є єдиною для усіх інформаційних задач НБУ і СЕП. Для підвищення ступеня захисту електронних розрахункових документів у СЕП використовуються додаткові засоби, включаючи бухгалтерський контроль. Технологічні та криптографічні засоби безпеки використовуються не тільки в СЕП, а й у всіх інформаційних задачах НБУ.

2.6. Для забезпечення контролю за виконанням вимог щодо захисту інформації у банківських установах, що є учасниками інформаційно-обчислювальної мережі НБУ, служби захисту інформації регіональних управлінь НБУ мають виконувати планові (а в разі потреби – і позапланові) перевірки всіх установ, що використовують засоби захисту інформації НБУ. Планові перевірки всіх банківських установ мають виконуватися не менше ніж 1 раз на рік.

За результатами перевірки складається акт перевірки (або довідка), у якому в разі виявлення недоліків мають бути встановлені строки їх усунення.

2.9. Забороняється передавати, навіть тимчасово, засоби захисту іншим установам або особам, у тому числі й іншим установам однієї юридичної особи.

2.10. У додатку 1 дано узагальнений перелік найбільш серйозних порушень в організації роботи з засобами захисту інформації НБУ.

3. Режимні вимоги до приміщень

3.1. Банківські установи, які є учасниками інформаційно-обчислювальної мережі НБУ та які використовують засоби захисту інформації НБУ, повинні виділити приміщення, де обробляються електронні банківські документи, працюють та зберігаються в неробочий час засоби захисту інформації, для яких обов'язковими є такі вимоги...

4. Принципи побудови криптографічного захисту інформації

4.1. Основною метою криптографічного захисту інформації в інформаційно-обчислювальній мережі НБУ є забезпечення конфіденційності та цілісності електронної банківської інформації, а також суворої автентифікації учасників СЕП і фахівців банківських установ, які беруть участь у підготовці та обробці електронних банківських документів...

5. Порядок отримання, зберігання та заміни криптоблока

6. Порядок отримання, зберігання та заміни електронної картки

6.1. Електронна картка для банківських установ, що розташовані за межами обласного центру, надсилається спецзв'язком у подвійному конверті або передається через відповідальну особу банківської установи. Для банківських установ, що розташовані в обласному центрі, картка передається через відповідальну особу банківської установи...

7. Порядок роботи з генератором ключів

8. Порядок зберігання та роботи з таємними ключами

9. Відповідальні за роботу із засобами криптозахисту...

10. Функціональні обов'язки відповідальних осіб

11. Організація діловодства з питань захисту інформації

12. Перевірка готовності банківської установи до включення в інформаційно-обчислювальну мережу НБУ

13. Повернення засобів криптозахисту

14. Особливий порядок роботи в СЕП НБУ і зберігання засобів криптозахисту

15. Перелік питань, що вимагають інформування служби захисту інформації регіонального управління НБУ...

16. Контрольно-перевірні заходи щодо організації захисту інформації в банківській установі

16.1. У повсякденній діяльності банківської установи організація контролю забезпечення захисту електронних банківських документів відповідно до вимог нормативних документів НБУ покладається на:

керівника банківської установи (особи, яка виконує його обов'язки);

заступника керівника банківської установи, який за своїми службовими обов'язками або за окремим наказом по банківської установі призначений відповідальним за організацію захисту електронних банківських документів.

17. Ведення архівів...

від 16 листопада 2000 р. № 451
Зареєстровано в Міністерстві юстиції України 24 листопада 2000 р.
за № 859/5080

Про затвердження Правил надання банками на письмову вимогу керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю інформації і документів

Правління Національного банку України
п о с т а н о в л я є:

1. Затвердити Правила надання банками на письмову вимогу керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю інформації і документів (далі – Правила), що додаються.

2. Департаменту пруденційного нагляду, Департаменту валютного контролю та ліцензування, іншим самостійним структурним підрозділам та територіальним управлінням Національного банку України забезпе-

чувати виявлення порушень законодавства з питань боротьби з організованою злочинністю з боку банків і притягнення винних осіб до відповідальності.

3. Зобов'язати банки неухильно і своєчасно виконувати письмові вимоги керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю щодо надання інформації і документів згідно з Правилами.

6. Контроль за виконанням цієї постанови покласти на заступника Голови, Департамент пруденційного нагляду, Департамент валютного контролю та ліцензування та керівників територіальних управлінь Національного банку України.

В.О. Голови А.В. Шаповалов

ЗАТВЕРДЖЕНО
Постанова Правління Національного банку України 16.11.2000 р. № 451
Зареєстровано
в Міністерстві юстиції України 24 листопада 2000 р. за № 859/5080

ПРАВИЛА
надання банками на письмову вимогу керівників
відповідних спеціальних підрозділів
по боротьбі з організованою злочинністю інформації і документів

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ці Правила встановлюють порядок надання банками інформації і документів про операції, рахунки, вклади фізичних осіб, за якими провадяться справи органами служби безпеки, внутрішніх справ, і юридичних осіб.

Дія цих Правил поширюється на інформаційні відносини, що виникають у сфері боротьби з організованою злочинністю, між банками і спеціальними підрозділами по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України.

1.2. Інформація і документи в цих Правилах – це зафіксовані на паперовому або іншому носії документовані відомості про операції, рахунки та вклади клієнтів і кореспондентів банку.

1.3. Основними завданнями цих Правил є:

створення сприятливих умов у сфері боротьби з організованою злочинністю з метою її попередження та ліквідації;

забезпечення необхідних умов для виконання банками обов'язків щодо надання інформації і документів спеціальним підрозділам по боротьбі з

організованою злочинністю органів внутрішніх справ і Служби безпеки України на письмову вимогу їх керівників згідно із законодавством, що регулює відносини в сфері боротьби з організованою злочинністю.

1.4. Спеціальні підрозділи по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України отримують від банків інформацію і документи на засадах та в межах повноважень, установлених чинним законодавством України.

2. ПОРЯДОК НАДАННЯ БАНКАМИ ІНФОРМАЦІЇ І ДОКУМЕНТІВ СПЕЦІАЛЬНИМ ПІДРОЗДІЛАМ ПО БОРОТЬБІ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ ОРГАНІВ ВНУТРІШНІХ СПРАВ, СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

2.1. Інформація і документи про операції, рахунки, вклади фізичних і юридичних осіб надаються банками спеціальним підрозділам по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України на письмову вимогу їх керівників або осіб, які їх заміщають.

Банки надають інформацію спеціальним підрозділам по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України тільки про операції, рахунки, вклади своїх клієнтів і кореспондентів.

Документи, що знаходяться у документообігу або архіві банку, надаються спеціальним підрозділам по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України в копіях, засвідчених у встановленому порядку.

2.2. Письмова вимога – це лист відповідного спеціального підрозділу по боротьбі з організованою злочинністю з вимогою щодо надання інформації і документів про операції, рахунки, вклади фізичних і юридичних осіб із зазначенням законних підстав для цієї вимоги за підписом керівника або особи, яка його заміщає в установленому порядку, на фірмовому бланку та зареєстрований належним чином.

2.3. Інформація і документи про операції, рахунки, вклади фізичних і юридичних осіб надаються банками негайно, а якщо це неможливо – протягом 10 діб. Також банки мають повідомити відповідному спеціальному підрозділу по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України причини неможливості негайного надання на їх письмову вимогу інформації і документів.

Інформація і документи про операції, рахунки, вклади клієнтів і кореспондентів надаються спеціальним підрозділам по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України за підписом керівника банку або особи, яка його заміщає в установленому порядку.

2.4. Керівники банків забезпечують документообіг за письмовими вимогами керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю та ведення архіву (на паперових або інших носіях) за наданими на ці вимоги інформацією і документами уповноваженими працівниками, а також визначають працівників банку, які матимуть доступ до такої інформації і документів.

2.5. Банки мають право оскаржити в порядку, установленому законодавством України, дії співробітників спеціальних підрозділів по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України, що вважають неправомірними.

Заступник директора Юридичного департаменту В.А. Сєнніков

від 28 грудня 2002 р. № 538
Зареєстровано в Міністерстві юстиції України 24 січня 2003 р. за № 56/7377

Про затвердження Положення про порядок здійснення Національним банком України наглядових функцій щодо банків, діяльність яких пов'язана з державною таємницею

Правління Національного банку України
п о с т а н о в л я є:

1. Затвердити Положення про порядок здійснення Національним банком України наглядових функцій щодо банків, діяльність яких пов'язана з державною таємницею (додається).

3. Контроль за виконанням цієї постанови покласти на заступника Голови, Генеральний департамент банківського нагляду та Департамент банківської безпеки.

Голова С.Л. Тігіпко

ПОГОДЖЕНО Голова Служби безпеки України В.І. Радченко

ЗАТВЕРДЖЕНО
Постанова Правління Національного банку України 28.12.2002 р. № 538
Зареєстровано
в Міністерстві юстиції України 24 січня 2003 р. за № 56/7377

ПОЛОЖЕННЯ
про порядок здійснення Національним банком України наглядових функцій щодо банків, діяльність яких пов'язана з державною таємницею

1. Загальні положення

1.1. Положення про порядок здійснення Національним банком України наглядових функцій щодо банків, діяльність яких пов'язана з державною таємницею (далі – Положення), розроблено на підставі Законів України «Про державну таємницю», «Про Національний банк України», «Про банки і банківську діяльність», інших законодавчих актів України, а також нормативно-правових актів Національного банку України (далі – Національний банк).

1.2. Положення визначає порядок здійснення Національним банком контрольно-наглядових функцій щодо банків та їх структурних підрозділів, діяльність яких пов'язана з державною таємницею (далі – банки).

1.3. У цьому Положенні терміни вживаються відповідно до їх значень, що встановлені Законом України «Про державну таємницю».

1.4. Право на отримання працівником (працівниками) Національного банку, який здійснює контрольно-наглядові функції, доступу до документів банку, що містять державну таємницю, надається згідно з приписом про виконання завдання (далі – припис, зразок якого подається в додатку до цього Положення), підписаним Головою Національного банку або особою, яка виконує його обов'язки.

1.6. Відповідальність за обґрунтованість викладеного в приписі завдання та обсяг відомостей, що становлять державну таємницю, з якими має ознайомитися працівник (працівники) Національного банку, покладається на посадову особу, яка підписує припис. Підпис цієї особи на приписі засвідчується гербовою печаткою.

1.7. Доступ працівника (працівників) Національного банку до секретної документації, що містить державну таємницю, у тому банку, у якому має здійснюватися перевірка, забезпечується з письмового дозволу керівника цього банку або особи, яка виконує його обов'язки, після пред'явлення цим працівником (працівниками) припису та довідки про допуск до державної таємниці (далі – довідка) за формою, що має відповідати ступеню секретності відомостей, з якими є потреба ознайомитися працівнику (працівникам) Національного банку.

1.8. Форма довідки та її реквізити мають відповідати державним зразкам, що встановлені згідно з діючими на час її заповнення нормативно-правовими актами України з питань охорони державної таємниці. Ця довідка може використовуватися для виконання завдань, пов'язаних із державною таємницею, як в одному, так і в кількох банках. Довідку видає режимно-секретний орган (далі – РСО) Національного банку за підписом його керівника, який засвідчується печаткою цього органу.

1.9. Перевірку банків, діяльність яких пов'язана з державною таємницею, здійснює працівник (працівники) Національного банку з дотриманням вимог законодавства України про державну таємницю та режиму секретності, що встановлений у банку, який перевіряється.

2. Порядок надання доступу до секретної інформації

2.1. У разі проведення Національним банком перевірки банку, діяльність якого пов'язана з державною таємницею, працівнику (працівникам) Національного банку слід пред'явити керівництву цього банку припис та довідку про допуск до державної таємниці за встановленими формами.

2.2. Працівнику (працівникам) Національного банку, який прибув до банку з метою проведення перевірки, надається доступ до секретних документів та відомостей банку, що становлять державну таємницю (далі – доступ до секретної інформації), лише в тих обсягах, які йому потрібні для виконання завдань, що зазначені в приписі.

2.3. Рішення про надання працівнику (працівникам) Національного банку доступу до секретної інформації з посиланням на перелік конкретних матеріалів (відомостей) оформляється керівником банку або особою, яка виконує його обов'язки (далі – керівник банку), як письмове розпорядження на зворотному боці припису. Рішення про надання доступу до секретної інформації може бути прийняте лише в разі пред'явлення працівником (працівниками) Національного банку відповідної довідки та припису.

2.4. Якщо керівник банку має обґрунтовані підстави для ненадання працівнику (працівникам) Національного банку права на доступ до секретної інформації, то він протягом трьох робочих днів зобов'язаний звернутися за роз'ясненнями до посадової особи, яка підписала припис, та повідомити про це відповідний орган (підрозділ) Служби безпеки України, який протягом місяця зобов'язаний прийняти рішення щодо обґрунтованості відмови банку в наданні такого доступу.

2.5. У разі позитивного вирішення питання про надання банком працівнику (працівникам) Національного банку доступу до секретної інформації згідно із записом на зворотному боці припису уповноважена

керівником банку особа має безпосередньо вирішувати питання щодо створення для працівника (працівників) Національного банку відповідних умов для роботи з секретною інформацією та її матеріальними носіями, дотримання ним установленого в банку режиму секретності.

2.6. Працівник (працівники) Національного банку, який здійснює перевірку, має право отримувати всі матеріальні носії секретної інформації, що зазначені в приписі (якщо інше в ньому не обумовлено), і зобов'язаний беззаперечно виконувати встановлені в банку вимоги режиму секретності.

2.7. Керівник банку може відмовити працівнику (працівникам) Національного банку, який здійснює перевірку, у наданні доступу до секретних відомостей у разі порушення ним вимог законодавства України про державну таємницю або умов, що визначені цим Положенням, а також за наявності інших обґрунтованих підстав для відмови.

2.8. Керівник банку протягом трьох робочих днів з дня відмови має повідомити про причини відмови в наданні працівнику (працівникам) Національного банку подальшого доступу до потрібної секретної інформації посадову особу Національного банку, яка підписала відповідний припис.

2.9. У разі виявлення фактів безпідставного вимагання працівником (працівниками) Національного банку секретних документів, що не стосуються мети та завдань перевірки та не зазначені в приписі, керівник банку має повідомити про це одночасно Національний банк і відповідний орган (підрозділ) Служби безпеки України.

3. Оформлення результатів перевірки банку

3.1. Працівник (працівники) Національного банку під час виконання ним своїх контрольно-наглядових функцій зобов'язаний виконувати вимоги цього Положення та вимоги банку щодо дотримання встановленого режиму секретності і правил ведення секретного діловодства. Він має право робити секретні записи лише в робочих зошитах (журналах), що надаються РСО банку, який перевіряється. У разі потреби РСО банку має надавати такі зошити (журнали) працівнику (працівникам) Національного банку, який проводить перевірку, за його запитом. У разі довгострокових перерв у роботі з секретними документами і після закінчення робочого дня зазначені зошити (журнали) мають повертатися в РСО банку.

Після закінчення перевірки робочі зошити (журнали) можуть (за рішенням працівника (працівників) Національного банку) відправлятися у встановленому порядку на адресу РСО Національного банку.

3.2. За результатами проведеної в банку перевірки працівник (працівники) Національного банку складає акт. У разі виникнення потреби включення до акта відомостей, що містять державну таємницю, йому

надається відповідний гриф секретності. У такому разі оформлення та пересилання акта здійснюються з дотриманням відповідних вимог законодавства про державну таємницю. Кількість примірників акта для належного виконання встановленого завдання визначає працівник (працівники) Національного банку, і вона має бути мінімальною.

3.3. Після того, як працівник (працівники) Національного банку закінчив свою роботу, керівник РСО банку в довідці про ознайомлення із секретними документами (зворотний бік припису) має зазначити, з якими конкретно документами або іншими матеріальними носіями секретної інформації ознайомлений працівник (працівники) Національного банку, а також ступінь секретності відомостей, що містяться в них. Цей запис обов'язково засвідчується підписом особи, яка його зробила, із зазначенням її посади, прізвища та ініціалів.

Кожна особа, яка зазначена в довідці про ознайомлення із секретними документами, засвідчує достовірність зроблених у ній записів своїм підписом із зазначенням прізвища, ініціалів та дати ознайомлення.

3.4. Припис разом з довідкою про ознайомлення із секретними документами зберігається в РСО банку протягом терміну, що визначається законодавством України про державну таємницю, залежно від ступеня секретності відомостей, з якими ознайомлювався працівник (працівники) Національного банку.

3.5. РСО банку після закінчення перевірки та заповнення працівником (працівниками) Національного банку довідки про ознайомлення із секретними документами зобов'язаний повернути пред'явлену йому довідку про допуск до державної таємниці із зазначенням на зворотному її боці грифа секретності документів, з якими був ознайомлений працівник (працівники) Національного банку під час виконання контрольно-наглядових функцій, та дати ознайомлення. Цей запис засвідчується підписом керівника РСО банку та відбитком печатки РСО банку.

3.6. Посадова особа Національного банку, яка підписала припис, через керівника банку може здійснювати контроль за роботою працівника (працівників) Національного банку щодо фактичного отримання ним доступу до секретної інформації, з якою він має працювати під час виконання контрольно-наглядових функцій.

3.7. Працівник (працівники) Національного банку, якому надано в банку, що перевіряється, доступ до секретної інформації, зобов'язаний у разі виникнення обставин, що перешкоджають збереженню державної таємниці, що стала йому відома у зв'язку з виконанням службових обов'язків, повідомити про це посадових осіб банку, які надали цей доступ, та РСО Національного банку.

3.8. Працівник (працівники) Національного банку, якому надано доступ до секретної інформації на період виконання контрольно-наглядових

функцій, у разі порушення ним законодавства про державну таємницю та встановленого в банку режиму секретності несе дисциплінарну та адміністративну відповідальність згідно із законодавством України.

Працівник (працівники) Національного банку, який винен у розголошенні державної таємниці, що стала йому відома у зв'язку з виконанням контрольно-наглядових функцій, несе кримінальну відповідальність.

Директор Генерального департаменту
банківського нагляду О.І. Кірєєв

НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ
ЛИСТ № 18-113/3105 від 17.08.2001

Национальный банк Украины рассмотрел письмо о предоставлении разъяснений некоторых положений законодательства Украины, касающихся раскрытия банковской тайны путем проведения обыска и выемки, и сообщает следующее.

Согласно части второй статьи 19 Конституции Украины органы государственной власти и органы местного самоуправления, их должностные лица обязаны действовать только на основании, в пределах полномочий и способом, предусмотренными Конституцией и законами Украины.

Информация о юридических и физических лицах, которая содержит банковскую тайну, раскрывается банками в соответствии с пунктами

1-4 части первой статьи 62 Закона Украины «О банках и банковской деятельности». То есть статья 62 указанного Закона предусматривает только непосредственные действия банка по раскрытию информации, содержащей банковскую тайну.

Проведение следователем процессуальных действий, в частности обыска и выемки, урегулировано Уголовно-процессуальным кодексом Украины.

Обыск и выемка должны проводиться на основаниях и в порядке, определенных главой 16 «Обыск и выемка» Уголовно-процессуального кодекса Украины.

Так, согласно статьям 177 и 178 УПК Украины выемка проводится по мотивированному постановлению следователя, а обыск, кроме того, – еще с санкции прокурора или его заместителя.

Согласно статье 183 УПК Украины перед обыском или выемкой следователь предъявляет постановление лицам, занимающим помещение, или представителю предприятия, учреждения или организации, где

проводятся обыск или выемка, и предлагает им выдать указанные в постановлении предметы или документы (в том числе содержащие банковскую тайну).

При этом должностные лица и граждане в соответствии с частью первой статьи 179 УПК Украины не имеют права отказываться предъявить или выдать указанные документы, которые требует следователь при обыске и выемке.

Учитывая изложенное, при проведении обыска и выемки, по нашему мнению, не происходит раскрытия информации, содержащей банковскую тайну, непосредственно банками. В этом случае документы, которые содержат банковскую тайну в отношении юридических или физических лиц, принудительно изымаются правоохранительными органами, и должностные лица банка не имеют права отказать следователю в предоставлении таких документов при проведении обыска и выемки.

Заместитель директора
Юридического департамента В.Рябец

«Бизнес – Бухгалтерия. Право. Налоги. Консультации», № 39 (454), 24 вересня 2001 р.

від 27.08.2001 № 367

Зареєстровано в Міністерстві юстиції України
15 листопада 2001 р. за № 954/6145

Положення
про порядок емісії платіжних карток і здійснення операцій з їх застосуванням

7.11. Платіжною організацією має бути розроблене Положення про внутрішньодержавну платіжну систему, що визначає правила її діяльності. Це Положення має визначати організаційну структуру платіжної системи, умови членства, порядок вступу та виходу з неї, опис платіжних засобів, правила виконання розрахунків за операціями з цими платіжними засобами, управління ризиками та ***безпекою в системі,*** порядок вирішення спорів та інше, визначене платіжною організацією.

від 30 квітня 2002 р. № 164
Про схвалення Методичних рекомендацій
з питань розроблення банками України програм
з метою протидії легалізації (відмиванню) грошей,
отриманих злочинним шляхом

Відповідно до Закону України «Про Національний банк України» та з метою реалізації статті 18 Закону України «Про фінансові послуги та державне регулювання ринків фінансових послуг», виконання статей 63 – 65 Закону України «Про банки і банківську діяльність», Указу Президента України від 10.12.2001 № 1199/2001 «Про заходи щодо запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом», а також пункту «С» «Роль фінансової системи у боротьбі з відмиванням грошей» Сорока рекомендацій Групи розробки фінансових заходів боротьби з відмиванням грошей (FATF), впроваджених спільною постановою Кабінету Міністрів України та Національного банку України від 28.08.2001 № 1124, та стандартів Базельського комітету банківського нагляду «Належне ставлення банків до клієнтів» Правління Національного банку України

п о с т а н о в л я є:

1. Схвалити Методичні рекомендації з питань розроблення банками України програм з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом (додаються).

3. Постанова набирає чинності з дня її підписання.

Голова В.С. Стельмах

СХВАЛЕНО Постанова Правління Національного банку України 30.04.2002 р. № 164

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
з питань розроблення банками України програм з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом

Програми протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, містять розроблення внутрішніх контролюючих процедур, програм здійснення внутрішнього контролю, організацію програм підготовки працівників та забезпечення надання інформації уповноваженим органам про значні та/або сумнівні операції та осіб, які їх здійснили.

Основним принципом розроблення програм внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, є забезпечення участі всіх працівників банку, незалежно від посади в межах їх компетенції, у виявленні операцій, що підлягають обов'язковому фінансовому контролю (далі

- обов'язковий контроль), та інших операцій з грошовими коштами або іншим майном, пов'язаних з легалізацією (відмиванням) грошей, отриманих злочинним шляхом.

1. Загальні положення

1.1. Відповідальним за організацію в банку протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, є керівник виконавчого органу банку (далі – керівник банку) або уповноважена ним особа.

1.2. Програми та інші документи з питань протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, затверджуються в порядку, що передбачений статутними документами банку.

1.3. Програми внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, розробляються з урахуванням таких положень:

а) необхідність збереження конфіденційної інформації про внутрішні документи банку;

б) необхідність збереження конфіденційної інформації про рахунки і внески клієнтів банку, про клієнтів і їх операції, а також інших відомостей, що становлять банківську таємницю;

в) виключення можливості залучення і співучасті працівників банку в здійсненні легалізації (відмивання) грошей, отриманих злочинним шляхом.

1.4. До операцій, що потребують обов'язкового контролю, належать значні та сумнівні операції, які визначені статтею 64 Закону України «Про банки і банківську діяльність». Критерії віднесення операцій до сумнівних визначаються Кабінетом Міністрів України. Також банкам рекомендовано контролювати сумнівні операції на підставі ознак, зазначених у додатку 1 до цих Методичних рекомендацій.

1.5. Внутрішній контроль з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, може містити порядок документарного фіксування необхідної інформації та забезпечення конфіденційності інформації, кваліфікаційні вимоги до підготовки і навчання кадрів, а також критерії виявлення і ознаки сумнівних операцій з урахуванням особливостей діяльності банку.

Програми внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, можуть містити також й інші програми та процедури.

2. Програми здійснення внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом

2.1. Програми здійснення внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, розробляються банком з урахуванням цих Методичних рекомендацій, а також особливостей організації, основних напрямів діяльності банку, клієнтської бази і рівня ризиків, пов'язаних з клієнтами і їх операціями, і містять:

а) програму здійснення ідентифікації і вивчення банком своїх клієнтів;

б) програму виявлення в діяльності клієнтів сумнівних операцій, що підлягають обов'язковому контролю, і інших операцій з грошовими коштами або іншим майном, що можуть бути пов'язані з легалізацією (відмиванням) грошей, отриманих злочинним шляхом;

в) програму перевірки інформації про клієнта або операцію клієнта для підтвердження обґрунтованості або спростування підозр стосовно здійснення клієнтом легалізації (відмивання) грошей, отриманих злочинним шляхом;

г) програму проведення документарного фіксування інформації, необхідної для ідентифікації клієнта та щодо здійснених ним операцій;

ґ) програму зберігання інформації і документів, отриманих у результаті реалізації програм здійснення внутрішнього контролю, з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом;

д) програму навчання працівників банку з питань протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом;

е) інші програми здійснення внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом.

2.2. Під час розроблення банком програми ідентифікації і вивчення банком своїх клієнтів рекомендується використовувати анкетування клієнта. Зразки анкет зазначені в додатку 2 до цих Методичних рекомендацій, а також:

а) банк ідентифікує і вивчає свого клієнта при проведенні банківських операцій і інших операцій відповідно до законодавства України та міжнародної практики шляхом отримання від клієнта потрібної інформації і документів.

Усі документи, що дають змогу ідентифікувати і вивчити клієнта, повинні бути дійсними на дату їх пред'явлення;

б) з метою ідентифікації резидентів банку рекомендується визначити...

г) банк при вивченні документів, зокрема статутних документів юридичної особи і документів, що підтверджують його державну реєстрацію, з метою більш ретельного вивчення свого клієнта, звертає особливу увагу на:

оформлення статутних документів (включаючи всі зареєстровані зміни) клієнта і документів, що підтверджують державну реєстрацію клієнта як юридичної особи;

склад засновників (учасників) юридичної особи, визначивши осіб, які мають можливість впливати на прийняття рішень органами юридичної особи, структуру органів управління юридичної особи і їх повноваження;

розмір зареєстрованого й оплаченого статутного капіталу або величину статутного фонду, майна;

ґ) якщо банк встановив, що від імені клієнта діє його представник, то банк його ідентифікує, перевіряє повноваження, а також ідентифікуг і вивчає клієнта, інтереси якого представляє;

д) якщо клієнт відкриває поточний чи/та депозитний рахунок (вносить внесок) на ім'я третьої особи, то банк має отримати від клієнта інформацію і документи, що дають змогу ідентифікувати і вивчити цю третю особу;

е) у разі встановлення кореспондентських відносин банк з'ясовує, у тому числі шляхом надсилання запиту кореспонденту, чи здійснюються кореспондентом банку заходи щодо протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, у тому числі ідентифікація і вивчення клієнтів.

Банку не рекомендується встановлювати кореспондентські відносини, якщо його кореспондентом не здійснюються заходи щодо протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом;

є) з метою концентрації зусиль щодо протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, на підставі всієї інформації і документів, що дають можливість ідентифікувати і вивчити клієнта, банку рекомендується оцінити ризик здійснення клієнтом легалізації (відмивання) грошей, отриманих злочинним шляхом.

Банку рекомендується розробити критерії оцінки ризику можливості здійснення клієнтом легалізації (відмивання) грошей, отриманих злочинним шляхом, за основу яких можуть бути взяті критерії, що визначені в додатку 3 до цих Методичних рекомендацій;

ж) банк поновлює відомості, отримані в результаті ідентифікації і вивчення клієнта, не рідше одного разу на рік у випадках, коли банк оцінює ризик здійснення клієнтом легалізації (відмивання) грошей, отриманих злочинним шляхом, як високий і не рідше ніж один раз у два роки в інших випадках;

з) якщо банк оцінює ризик здійснення клієнтом легалізації (відмивання) грошей, отриманих злочинним шляхом, як високий, то банк приділяє підвищену увагу операціям, що проводяться за рахунками клієнта, та з метою перевірки інформації про клієнта може направити свого працівника, який відповідає за роботу з цим клієнтом, на місце здійснення діяльності клієнта.

2.3. Під час розроблення програми виявлення в діяльності клієнтів операцій, що підлягають обов'язковому контролю, і інших операцій з грошовими коштами або іншим майном, пов'язаних з легалізацією (відмиванням) грошей, отриманих злочинним шляхом, банк визначає для себе критерії виявлення і ознаки сумнівних операцій з урахуванням вимог законодавства України та міжнародної практики. За основу можуть бути взяті критерії виявлення і ознаки сумнівних операцій, що визначені в додатку 1 до цих Методичних рекомендацій.

2.4. Під час розроблення програми перевірки інформації про клієнта або операцію клієнта для підтвердження обґрунтованості або спростування підозр здійснення клієнтом легалізації (відмивання) грошей, отриманих злочинним шляхом, банку рекомендується встановити таку процедуру:

а) у разі кваліфікації операції клієнта як сумнівної працівник банку, який виявив цю операцію, складає Повідомлення – документ, що містить відомості про операцію (операції). Банку рекомендується розробити форму Повідомлення, що містить реквізити, зазначені в додатку 4 до цих Методичних рекомендацій.

Повідомлення передається відповідальній особі (далі – відповідальний працівник), яка забезпечує реалізацію внутрішнього контролю в порядку, встановленому в розділі 3 цих Методичних рекомендацій;

б) відповідальний працівник приймає остаточне рішення про визнання операції клієнта сумнівною, що підлягає обов'язковому контролю, і надання відомостей про неї до уповноваженого органу;

в) у разі виявлення сумнівних операцій відповідальний працівник приймає рішення про подальші дії банку щодо клієнта і його операції;

г) у разі виявлення в діяльності клієнта сумнівної операції банк може зробити такі дії:

звернутися до клієнта з проханням про надання необхідних пояснень, у тому числі додаткових відомостей, що роз'яснюють економічне значення сумнівної операції;

забезпечити підвищену увагу (відповідно до цих Методичних рекомендацій) до всіх операцій (угод) клієнта, що здійснюються через банк;

провести інші дії за умови дотримання законодавства України;

ґ) про будь-яке рішення відповідального працівника стосовно операції (угоди) робиться відповідний запис (відмітка) в Повідомленні.

2.5. Банк під час розроблення програми проведення документарного фіксування інформації, необхідної для ідентифікації клієнта та щодо здійснених ним операцій, банк фіксує:

а) інформацію про операції (угоди) клієнта таким чином, щоб у разі потреби можливо було відтворити деталі операції (угоди), в тому числі суму операції (угоди), валюту платежу, дані про контрагента тощо;

б) інформацію про клієнта і збирає документи з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, таким чином, щоб вони могли бути використані як доказ у кримінальному, цивільному і господарському процесах.

2.6. Під час розроблення програми зберігання інформації і документів, отриманих у результаті реалізації програм здійснення внутрішнього контролю, з метою протидії легалізації (відмивання) грошей, отриманих злочинним шляхом, банку рекомендується зберігати такі документи:

копії документів, що містять відомості про клієнта, або їх реквізити – не менше ніж п'ять років після припинення зобов'язань між банком і клієнтом;

оригінали або копії щодо проведеної операції (операцій), які можуть бути використані як доказ в кримінальному, цивільному і господарському процесах, а також Повідомлення – протягом не менше ніж п'ять років після здійснення відповідної операції (операцій). Облік і зберігання Повідомлень здійснює відповідальний працівник у встановленому банком порядку;

інші документи, у тому числі ділове листування – не менше ніж п'ять років після припинення зобов'язань між банком і клієнтом.

2.7. Під час розроблення програми навчання працівників банку з питань протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, банк організовує навчання працівників, виходячи з їх посадових обов'язків, за такими напрямами:

а) ознайомлення працівників з нормативно-правовими актами у сфері протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом;

б) ознайомлення працівників з правилами внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, затвердженими банком;

в) практичні заняття щодо реалізації програм внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, у тому числі програм його здійснення.

Програма навчання будується виходячи з того, що основною умовою успішного здійснення банком діяльності щодо протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, є безпосередня участь кожного працівника в межах його компетенції в цьому процесі.

Навчання працівників банку з питань протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, проводяться не рідше ніж один раз на рік.

3. Організація в банку роботи щодо протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом

Під час організації в банку роботи щодо протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, рекомендується здійснювати такі заходи.

3.1. Керівник банку призначає відповідального працівника, який відповідатиме за розроблення та реалізацію правил внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, і за порядок їх здійснення, а також інших внутрішніх організаційних заходів.

Відповідальний працівник має бути незалежним у своїй діяльності від інших структурних підрозділів банку і підзвітний тільки керівнику банку.

3.2. У банку з урахуванням особливостей його організації, основних напрямів його діяльності, клієнтської бази і рівня його ризиків, пов'язаних з клієнтами і їх операціями, може бути сформовано або визначено окремий структурний підрозділ з протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, під керівництвом відповідального працівника.

Зазначений підрозділ функціонує відповідно до положення про цей структурний підрозділ, що затверджується згідно з внутрішніми процедурами банку.

3.3. З метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, відповідальний працівник здійснює такі функції:

а) організовує розроблення та подає на затвердження керівнику банку правила внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, і порядок його здійснення;

б) організовує реалізацію правил внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, у тому числі порядок їх здійснення. У зв'язку з цим він:

консультує працівників банку з питань, що виникають під час реалізації програм здійснення внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, у тому числі при ідентифікації і вивченні клієнтів банку й оцінці ризику здійснення клієнтом легалізації (відмивання) грошей, отриманих злочинним шляхом;

приймає рішення щодо поданих йому повідомлень;

організовує роботу щодо навчання працівників банку з питань протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом;

в) організовує надання до уповноваженого органу інформації про значні та/або сумнівні операції відповідно до статті 64 Закону України «Про банки і банківську діяльність»;

г) сприяє уповноваженим представникам Національного банку під час проведення ними інспекційних перевірок діяльності банку з питань, віднесених до його компетенції;

ґ) не рідше ніж один раз на рік подає письмовий звіт про результати реалізації правил внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, та порядку його

здійснення, керівнику банку. Порядок поточної звітності відповідального працівника визначається внутрішніми документами банку;

д) виконує інші функції відповідно до цих Методичних рекомендацій і внутрішніх документів банку.

3.4. Під час здійснення своїх функцій відповідальний працівник має право:

а) отримувати від керівників і працівників підрозділів банку необхідні документи, у тому числі накази й інші розпорядчі документи, видані керівництвом банку і його підрозділами; бухгалтерські, касові та грошово-розрахункові документи тощо;

б) робити копії з отриманих документів, у тому числі копії файлів, будь-яких записів, що зберігаються в локальних обчислювальних мережах і автономних комп'ютерних системах;

в) входити до приміщень підрозділів банку, а також до приміщень, в яких зберігаються документи (архіви), здійснюється комп'ютерне оброблення даних і зберігання даних на машинних носіях (комп'ютерні зали);

г) видавати тимчасові у межах термінів, встановлених законодавством України для проведення операції (до рішення керівника банку), розпорядження про припинення проведення операції з метою отримання додаткової або перевірки наявної інформації про клієнта або операцію;

ґ) інші права відповідно до цих Методичних рекомендацій і внутрішніх документів банку.

3.5. Під час здійснення своїх функцій відповідальний працівник зобов'язаний:

а) забезпечувати збереження і повернення отриманих від відповідних підрозділів банку документів;

б) забезпечувати конфіденційність інформації, отриманої під час здійснення відповідальним працівником своїх функцій;

в) виконувати інші обов'язки відповідно до цих Методичних рекомендацій і внутрішніх документів банку.

3.6. Здійснення функцій, встановлених цими Методичними рекомендаціями і внутрішніми документами банку, належить до виняткової компетенції відповідального працівника.

Працівники структурного підрозділу з протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, можуть здійснювати функції, зазначені в підпункті «б» пункту 3.3, мають права, наведені в підпунктах «а» – «в» пункту 3.4, і виконують обов'язки, зазначені в підпункті 3.5 цих Методичних рекомендацій.

3.7. Банку рекомендується не покладати на відповідального працівника здійснення інших функцій, що не відповідають його основним функціям.

3.8. Банк визначає кваліфікаційні вимоги до відповідального працівника і працівників підрозділу з протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом (за його наявності), з урахуванням вимог, визначених у додатку 5 до цих Методичних рекомендацій.

3.9. Працівники підрозділів банку сприяють відповідальному працівнику (працівникам очолюваного ним структурного підрозділу) у здійсненні ним своїх функцій відповідно до вимог цих Методичних рекомендацій і внутрішніх документів банку.

3.10. Керівником банку встановлюється порядок взаємодії працівників банку з відповідальним працівником.

3.11. У разі виникнення в працівників банку питань під час реалізації внутрішнього контролю для протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, вони звертаються за консультацією до відповідального працівника.

3.12. З метою моніторингу за процесом функціонування в банках системи внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, службі внутрішнього аудиту банку рекомендується виконувати такі функції:

а) здійснювати внутрішній контроль за відповідністю діяльності банку, а також його працівників, законам, нормативно-правовим актам України у сфері боротьби з легалізацією (відмиванням) грошей, отриманих злочинним шляхом;

б) здійснювати контроль за дотриманням працівниками банку правил внутрішнього контролю з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, затверджених банком.

3.13. Працівники банку, у тому числі відповідальний працівник, яким стали відомі факти порушень нормативно-правових актів у сфері протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом, які допущені працівниками банку під час проведення операції (операцій), негайно в письмовій формі їх доводять до відома свого безпосереднього керівника і служби внутрішнього контролю.

4. Порядок надання банком до уповноваженого органу інформації про значні та/або сумнівні операції та осіб, які їх здійснили

4.1. Рішення про надання уповноваженим органам інформації про значні та/або сумнівні операції та інформації про осіб, які їх здійснили (далі – інформація), приймається керівником банку на підставі Повідомлення з відміткою відповідального працівника.

4.2. Керівник банку приймає рішення про надання інформації протягом двох робочих днів з часу здійснення значної операції або віднесення відповідальним працівником операції до категорії сумнівної.

4.3. Перелік рекомендованих реквізитів для формування повідомлення уповноважених органів про значні та/або сумнівні операції і щодо осіб, які здійснили ці операції, зазначений у додатку 6 до цих Методичних рекомендацій.

4.4. Банкам рекомендується надавати інформацію на адресу відповідних органів, що зазначені в Законі України «Про організаційно-правові основи боротьби з організованою злочинністю», а саме:

а) управлінь по боротьбі з організованою злочинністю ГУ УМВС України в Автономній Республіці Крим, областях, містах Києві та Севастополі;

б) відділів по боротьбі з корупцією та організованою злочинністю органів Служби безпеки України в Автономній Республіці Крим, областях, містах Києві та Севастополі.

4.5. Інформацію рекомендується надавати вищезазначеним органам за місцезнаходженням банку на паперових носіях способами, які забезпечуватимуть їх гарантовану доставку і конфіденційність, наприклад, шляхом передавання запечатаного пакета з інформацією підприємству зв'язку чи іншому спеціалізованому підприємству для відправлення засобами спецзв'язку (кур'єрською, фельд'єгерською поштою тощо) згідно з Правилами приймання, оброблення та доставки кореспонденції банківських установ спецзв'язком Державного комітету зв'язку та інформатизації України, або шляхом доставляння пакета представником банку або його передавання підприємству зв'язку для відправлення рекомендованим чи цінним листом відповідно до Правил користування послугами поштового зв'язку України.

Додаток 1
до Методичних рекомендацій з питань розроблення банками України програм з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом

Критерії виявлення і ознаки сумнівних операцій

1. Загальні ознаки, що можуть свідчити про здійснення легалізації (відмивання) грошей, отриманих злочинним шляхом

1.1. Немотивована відмова в наданні клієнтом відомостей (не передбачених законодавством України) на запит банку відповідно до банківської практики, що склалася, а також зайва заінтересованість клієнта в нерозголошенні конфіденційної інформації щодо здійснюваної операції.

1.2. Зневага клієнтом більш вигідних умов надання послуг (тариф комісійної винагороди, ставки за строковими внесками (депозитами) і внесками (депозитами) до запитання тощо), а також пропозиція клієнта

щодо стягнення значно високої комісії або такої, що суттєво відрізняється від комісії, яка звичайно стягується при наданні таких послуг.

1.3. Операції клієнта не мають явного економічного сенсу, не відповідають характеру діяльності клієнта і не мають на меті управління ліквідністю або страхування ризиків.

1.4. Наявність нестандартних або значно складних інструкцій з порядку проведення розрахунків, що відрізняються від звичайної практики, яка використовується клієнтом, або від звичайної ринкової практики.

1.5. Необґрунтована терміновість у проведенні операції, на якій наполягає клієнт.

1.6. Внесення клієнтом у раніше узгоджену схему проведення операції (операцій) безпосередньо перед початком її реалізації значних змін, що особливо стосуються напряму руху грошових коштів або іншого майна.

1.7. Передавання клієнтом доручення про здійснення операції через представника (посередника), якщо представник (посередник) виконує доручення клієнта без встановлення прямого (особистого) контакту з банком.

1.8. Явна невідповідність операцій, що проводяться клієнтом з участю банку, загальноприйнятій ринковій практиці здійснення операцій.

1.9. Зарахування на рахунок клієнта на одній підставі від одного або кількох контрагентів сум коштів, що не перевищують окремо суму, еквівалентну 50000 євро, але внаслідок додавання (якби кошти були зараховані на основі одного платіжного документа) перевищують зазначену суму (за умови, що діяльність клієнта не пов'язана з обслуговуванням населення, збором обов'язкових або добровільних платежів), з подальшим переказом коштів на рахунок клієнта, що відкритий в іншому банку, або використанням коштів на купівлю іноземної валюти, цінних паперів й інших високоліквідних активів.

1.10. Дроблення сум грошових коштів, які перераховуються клієнтом одному або кільком контрагентам на одній підставі, протягом невеликого періоду часу, за умови, що сума перерахованих грошових коштів (якби вони були перераховані на підставі одного платіжного документа) перевищує суму, еквівалентну 50000 євро.

1.11. Відсутність інформації про клієнта (юридичної особи, у тому числі банку) в офіційних довідкових виданнях, а також неможливість встановити зв'язок з клієнтом за зазначеними адресами і телефонами.

1.12. Відсутність інформації про клієнта в банках, що його обслуговують або раніше обслуговували.

1.13. Труднощі, що виникають у банку під час перевірки інформації, що надається клієнтом відповідно до цих Методичних рекомендацій і внутрішніх документів банку, невиправдані затримки в поданні клієнтом

документів і інформації, представлення клієнтом інформації, яку неможливо перевірити, або ця перевірка дуже дорого коштує.

1.14. Неможливість встановлення контрагентів клієнта.

1.15. Відсутність очевидного зв'язку між характером і родом діяльності клієнта з послугами, з якими клієнт звертається до банку.

2. Ознаки, що можуть свідчити про здійснення легалізації (відмивання) грошей, отриманих злочинним шляхом, під час проведення операцій з готівкою і переказів грошових коштів

2.1. Відкриття протягом короткого часу на ім'я одного клієнта кількох строкових депозитних рахунків на суму, що не перевищує суму, еквівалентну 10000 євро для операції з готівкою та 50000 євро для безготівкової операції (крім випадків, коли відомо, що клієнт, виходячи з характеру його діяльності, регулярно протягом певного терміну отримує такі суми коштів), з подальшим зарахуванням сум після закінчення терміну внесків (депозитів) на один рахунок і/або подальшим переказом в інший банк.

2.2. Зарахування на рахунок клієнта значної кількості платежів від фізичних осіб на суму, що не перевищує суму, еквівалентну 10000 євро для операції з готівкою та 50000 євро для безготівкової операції, у тому числі через касу банку, якщо діяльність клієнта не пов'язана з наданням послуг населенню, збором обов'язкових або добровільних платежів.

2.3. Зарахування грошових коштів на рахунок клієнта – юридичної особи, операції за яким не здійснювалися протягом більше ніж три місяці або були незначними для цього клієнта, з подальшим зняттям клієнтом коштів у готівковій формі.

2.4. Регулярне зарахування на рахунок клієнта коштів у готівковій формі, у тому числі на основі прибуткового касового ордера, з подальшим переказом усієї або більшої частини суми навіть, якщо сума менша за суму, еквівалентну 50000 євро, протягом одного операційного дня, або наступного за ним дня на рахунок клієнта, відкритий в іншому банку, або на користь третьої особи, у тому числі нерезидента.

2.5. Переказ грошових коштів на анонімний (номерний) рахунок за кордон і надходження грошових коштів з анонімного (номерного) рахунку з-за кордону.

2.6. Регулярне представлення чеків, емітованих банком-нерезидентом і індосованих нерезидентом, на інкасо, якщо така діяльність не відповідає діяльності клієнта, відомій банку.

2.7. Не пов'язане прямо з діяльністю клієнта несподіване істотне збільшення сальдо на рахунку, яке згодом переводиться в інший банк або використовується для цілей купівлі іноземної валюти (з переказом на користь нерезидента), цінних паперів на пред'явника.

2.8. Істотне збільшення частки готівки, що надходить на рахунок клієнта – юридичної особи, якщо звичайними для основної діяльності клієнта є розрахунки в безготівковій формі.

2.9. Переказ грошових коштів з рахунку клієнта – юридичної особи на його рахунок в інший банк без наявної підстави (зокрема без закриття рахунку; не з метою погашення кредиту, отриманого від іншого банку; з призначенням платежу «переказ власних коштів»).

2.10. Нерегулярне або одноразове використання клієнтом рахунку для отримання грошових коштів з подальшим їх зняттям у готівковій формі на суму, що менша від суми, еквівалентної 10000 євро, з подальшим закриттям рахунку або припиненням за ним операцій.

2.11. Обмін значної суми банкнот, особливо іноземної валюти, низьких номіналів на банкноти вищих номіналів.

2.12. Розміщення на рахунку значної суми готівкових коштів клієнтом, який за рівнем доходу чи сферою діяльності не може здійснювати операцію на таку суму.

2.13. Систематичне повне зняття клієнтом значних сум готівки в день її надходження на його рахунок.

3. Ознаки, що можуть свідчити про здійснення легалізації (відмивання) грошей, отриманих злочинним шляхом, під час проведення операцій за кредитними договорами

3.1. Надання кредиту під забезпечення виконання зобов'язання, його повернення шляхом розміщення на рахунку, відкритому в банку кредитора або в іншому банку, грошових коштів у валюті кредиту, іншій валюті або цінних паперів на пред'явника.

3.2. Погашення простроченої заборгованості за кредитним договором, якщо умови діяльності клієнта та інформація, якою щодо цього клієнта володіє банк, не дають можливості встановити джерела фінансування погашення заборгованості.

3.3. Надання кредиту під заставу дорогоцінного каміння, увезеного на територію України, включаючи кредитування під заставу цих цінностей з розміщенням у сховищі кредитора, крім випадків кредитування підприємств, що здійснюють оброблення дорогоцінного каміння іноземного виробництва.

3.4. Надання кредиту під забезпечення у вигляді гарантії банку-нерезидента на суму, що становить ціле число (100 тисяч, один мільйон і тощо), за умови відсутності очевидного зв'язку між місцем діяльності клієнта і його контрагентів і місцезнаходженням гаранта особливо, якщо гарантія видається філією банку-нерезидента.

3.5. Інформація, що зазначена в заяві клієнта про надання кредиту, не відповідає відомостям і документам, отриманим під час проведення переговорів від представників клієнта.

3.6. У погашення кредиту клієнта надходять кошти із незазначених клієнтом або невідомих джерел погашення.

3.7. Надання або отримання кредиту з процентною ставкою, що істотно перевищує середню процентну ставку за кредитами на внутрішньому і зовнішньому ринках.

4. Ознаки, що свідчать про можливе здійснення легалізації (відмивання) грошей, отриманих злочинним шляхом, під час проведення міжнародних розрахунків

4.1. Сплата резидентом нерезиденту неустойки (пені, штрафу) за невиконання договору поставки товарів (виконання робіт, надання послуг) або за порушення умов договору, якщо розмір неустойки перевищує 10 % від суми непоставлених товарів (невиконаних робіт, ненаданих послуг).

4.2. Використання клієнтом міжнародних форм розрахунків, що не відповідають характеру основної діяльності клієнта (на основі даних про основну діяльність клієнта, що є в розпорядженні банку).

4.3. Одержувачем грошових коштів або товарів (робіт, послуг, результатів інтелектуальної діяльності) є нерезидент, що не є однією зі сторін за договором (контрактом), що передбачає імпорт (експорт) резидентом товарів (робіт, послуг, результатів інтелектуальної діяльності).

4.4. У договорі (контракті) передбачені експорт резидентом товарів (робіт, послуг, результатів інтелектуальної діяльності) або платежі за імпортом товарів (робіт, послуг, результатів інтелектуальної діяльності) на користь нерезидентів, зареєстрованих у державах і на територіях, що надають пільговий податковий режим, або не співпрацюють з Групою з розробки фінансових заходів боротьби з відмиванням грошей (FATF).

4.5. Товаросупровідні документи, що подані до банку за зовнішньоекономічними договорами (контрактами), за якими оформлені документи експортних (імпортних) операцій, не містять чіткого опису товарів, що є предметом зовнішньоекономічних контрактів.

5. Ознаки, що можуть свідчити про здійснення легалізації (відмивання) грошей, отриманих злочинним шляхом, під час проведення операцій з цінними паперами і похідними фінансовими інструментами

5.1. Регулярне укладення клієнтом строкових угод або використання інших похідних фінансових інструментів, особливо таких, що не передбачають поставки базового активу, за операціями з одним або кількома контрагентами, результатом чого є постійний прибуток або постійні збитки клієнта.

5.2. Разовий продаж (купівля) клієнтом великого пакета цінних паперів, що вільно не обертаються на організованому ринку, за цінами, істотно відмінних від ринкових, за умови, що клієнт не є професійним учасником

ринку цінних паперів і цінні папери не передаються клієнту в погашення простроченої заборгованості контрагента перед клієнтом.

5.3. Регулярні операції з купівлі з подальшим продажем цінних паперів, що не мають котирування і не обертаються вільно на організованому ринку цінних паперів, за умови, що прибуток від реалізації цінних паперів спрямований на придбання високоліквідних цінних паперів, що вільно обертаються на організованому ринку.

5.4. Одночасне виставляння клієнтом доручень на купівлю і продаж цінних паперів й інших фінансових інструментів за цінами, що мають помітне відхилення від поточних ринкових цін за аналогічними угодами.

5.5. Здійснення операцій, за яких один і той же самий фінансовий інструмент багато разів продається і потім викуповується під час проведення операцій з однією і тією ж стороною.

5.6. Проведення операцій з цінними паперами на пред'явника, не розміщеними в депозитаріях.

6. Ознаки, що можуть свідчити про здійснення легалізації (відмивання) грошей, отриманих злочинним шляхом, під час здійснення електронного банкінга і розрахунків за пластиковими картками

6.1. Регулярне переказування клієнтом грошових коштів на суму, що менша від суми, еквівалентної 50000 євро, одному або кільком контрагентам під час купівлі (продажу) товарів (робіт, послуг) за допомогою мережі інтернет з використанням кредитної (дебетної) картки з наданням права на списання коштів з рахунку клієнта.

6.2. Регулярне зарахування клієнтом, що надає послуги у сфері торгівлі за допомогою мережі інтернет, грошових коштів на суму, що менша суми, еквівалентної 50000 євро, яка надходить з рахунків для розрахунків з використанням кредитних (дебетних) карток клієнтів інших банків.

6.3. Регулярне зняття держателем кредитної або дебетної картки грошових коштів у готівковій формі через касу банку або через банкомат на суму, що менша від суми, еквівалентної 10000 євро (на підставі даних за операціями з пластиковими картами, що регулярно направляються через організацію, яка здійснює процесинг пластикових карток). Виключенням є зняття грошових коштів, що надійшли на рахунок працівника від роботодавця і що являють собою виплату роботодавцем своїм працівникам будь-яких форм матеріальної винагороди.

Додаток 3
до Методичних рекомендацій з питань розроблення банками України програм з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом

Критерії оцінки ризику можливості здійснення клієнтом легалізації (відмивання) грошей, отриманих злочинним шляхом

1. Види діяльності, яким притаманний високий ризик здійснення легалізації (відмивання) доходів, отриманих злочинним шляхом

1.1. Діяльність юридичних осіб (їх відокремлених підрозділів), які не є банками, що займаються переказом грошових коштів, платежами в готівковій формі за чеками, інкасацією грошових коштів, обміном валют на підставі агентських угод.

1.2. Діяльність юридичних осіб (у тому числі банків), зареєстрованих в офшорних зонах, їх відокремлених підрозділів, дочірніх і від них залежних підприємств.

1.3. Туристична діяльність (туроператорська і турагентська діяльність, а також інша діяльність з організації подорожей).

1.4. Гральний бізнес.

1.5. Діяльність, що пов'язана з реалізацією предметів мистецтва та антикваріату (у тому числі комісійна).

1.6. Здійснення зовнішньоекономічних операцій.

1.7. Торгівля (особливо експорт) дорогоцінними металами і дорогоцінним камінням, а також ювелірними виробами, що містять дорогоцінні метали і дорогоцінне каміння.

1.8. Торгівля (посередництво в торгівлі) нерухомим майном, автомобільним транспортом.

1.9. Будь-яка інша діяльність, що пов'язана з інтенсивним обігом готівки (у тому числі надання послуг у сфері роздрібної торгівлі, громадського харчування, роздрібна торгівля пальним на бензоколонках і газозаправних станціях тощо).

2. Географічний чинник – райони високого ризику здійснення легалізації (відмивання) доходів, отриманих злочинним шляхом

2.1. Держави (території), про яких з міжнародних джерел відомо, що вони не дотримуються загальноприйнятих стандартів у боротьбі з легалізацією (відмиванням) доходів, отриманих злочинним шляхом, або є державами (територіями) з підвищеним рівнем злочинності і корупції.

2.2. Держави (території), що сприяють діяльності терористичних груп.

2.3. Держави (території), де не передбачене розкриття або надання інформації під час проведення фінансових операцій.

2.4. Держави (території), що не виконують рекомендації Групи розробки фінансових заходів боротьби з відмиванням грошей (FATF).

2.5. Держави (території), в яких відбуваються військові дії.

2.6. Офшорні території.

3. Банківські операції (продукти) з високим ризиком використання для легалізації (відмивання) доходів, отриманих злочинним шляхом

3.1. Банківські операції (продукти), що дають змогу клієнтам легко конвертувати кошти з готівкової форми в безготівкову або за короткий час переказувати кошти з однієї держави в іншу.

Додаток 5
до Методичних рекомендацій з питань розроблення банками України програм з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом

Кваліфікаційні вимоги до відповідального працівника і працівників структурного підрозділу з протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом

1. До відповідального працівника рекомендується пред'являти такі вимоги:

1.1. Наявність вищої юридичної або економічної освіти і досвіду керівництва підрозділом банку, що здійснює банківські операції, не менше ніж один рік, а за відсутності спеціальної освіти – досвід керівництва таким підрозділом не менше двох років.

1.2. Відсутність судимості.

1.3. Наявність досвіду роботи в підрозділах з обслуговування клієнтів і в інших підрозділах банку, що здійснюють банківські операції й інші операції відповідно до законодавства України.

2. До працівників підрозділу з протидії легалізації (відмиванню) доходів, отриманих злочинним шляхом, рекомендується пред'являти такі вимоги:

2.1. Наявність вищої юридичної або економічної освіти і досвіду роботи в банку не менше ніж один рік, а за відсутності спеціальної освіти – досвід роботи в банку не менше двох років.

2.2. Відсутність судимості.

2.3. Наявність досвіду роботи в підрозділах з обслуговування клієнтів і в інших підрозділах банку, що здійснюють банківські операції й інші операції відповідно до законодавства України.

БІБЛІОГРАФІЯ

1. Конституція України.
2. Кримінальний Кодекс України.
3. Науково-практичний коментарій до Кримінального кодексу України. – К.: Юрінком, 2002.
4. Закон Української РСР «Про банки і банківську діяльність«, прийнятий Верховною Радою України 7 грудня 2000 року.
5. Закон України «Про Національний банк України» від 20 травня 1999 р. № 679-XIV.
6. Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» від 30 червня 1993 р. //Голос України. – 1994 . – 1 квітня.
7. Закон України «Про внесення змін до деяких законів України з питань запобігання використанню банків та інших фінансових установ з метою легалізації (відмивання) доходів, одержаних злочинним шляхом» від 6 лютого 2003 р. № 485-IV.
8. Закон України «Про інформацію» від 2 жовтня 1992 р.
9. Закон України «Про державну таємницю» від 21 січня 1994 р. № 3855-XII.
10. Закон України «Про підприємства в Україні» від 27 березня 1991. – № 887-XII.
11. Закон України «Про захист інформації в автоматизованих системах» від 5 липня 1994. – № 80/94-ВР.
12. Закон України «Про господарські товариства» від 19 вересня 1991 р. № 1576-XII.
13. Закон України «Про захист від недобросовісної конкуренції» від 7 червня 1996.
14. Закон України «Про аудиторську діяльність» від 22 квітня 1993 р. № 3125-XII.
15. Закон України «Про основи національної безпеки України» від 19 червня 2003. – № 964-IV.
16. Закон України «Про оперативно-розшукову діяльність» від 18 лютого 1992 р. № 2135-XII.

17. Закон України «Про контррозвідувальну діяльність» від 26 грудня 2002 р. № 374-IV.

18. Закон України «Про Службу безпеки України» від 25 березня 1992. – № 2229-XII.

19. Закон України «Про міліцію» від 20 грудня 1990. № 565-XII.

20. Закон України «Про прокуратуру» від 5 листопада 1991. № 1789-XII.

21. Закон УРСР «Про державну податкову службу в Українській РСР від 4 грудня 1990 р. № 509-XII».

22. Закон України «Про місцеве самоврядування в Україні» від 21 травня 1997. № 280/97-ВР.

23. Закон України «Про відновлення платоспроможності боржника або визнання його банкрутом» від 14 травня 1992 р. № 2343-XII.

24. Закон України Про внесення змін і доповнень до Закону України «Про банкрутство» від 25 лютого 1994 р. № 4036-XII.

25. Закон України Про внесення змін до Закону України «Про банкрутство» від 30 червня 1999 р. № 784-XIV .

26. Закон «Про державне регулювання ринку цінних паперів в Україні» від 30 жовтня 1996 р. № 448/96-ВР.

27. Закон України «Про заставу».

28. Закон України «Про лізинг» від 16 грудня 1997 р. № 723/97-ВР.

29. Закон України «Про електронні документи та електронний документообіг».

30. Закон України «Про електронний цифровий підпис».

31. Указ Президента України «Про невідкладні додаткові заходи щодо посилення боротьби з організованою злочинністю і корупцією» від 6 лютого 2003 р. № 84/2003.

32. Указ Президента України «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14 липня 2000 р. № 891/2000.

33. Указ Президента України «Про деякі питання захисту банківської таємниці» від 21 липня 1998.

34. Указ Президента України № 679 «Про відкриття анонімних валютних рахунків фізичних осіб (резидентів і нерезидентів)», який втратив чинність від 1 серпня 1995 р.

35. Постанова Кабінету Міністрів України № 1280 «Про впровадження механізму страхування експортних та кредитних ризиків» від 17 серпня 1998 р.

36. Постанова Правління Національного банку України від 18 грудня 1998 р. № 527 , якою затверджена «Інструкція про відкриття банками рахунків у національній та іноземній валюті» //Офіційний вісник України. – 2000. – № 19.

37. Постанова Правління Національного банку України № 601 «Про внесення змін до нормативно-правових актів Національного банку України з питань кредитування в іноземній валюті» від 22 грудня 1999 р. // Офіційний вісник України. – 2000. – № 2.

38. Постанова Правління Національного банку України № 602 «Про затвердження Положення про порядок реєстрації договорів, які передбачають виконання резидентами боргових зобов'язань перед нерезидентами, залученими від нерезидентів кредитами, позиками в іноземній валюті» від 22 грудня 1999 р.//Офіційний вісник України. – 2000. – № 2.

39. Постанова Правління Національного банку України № 587 «Про створення належних умов органам Державної податкової адміністрації України щодо контролю з питань оподаткування, належного забезпечення коштів до Державного бюджету України та вдосконалення порядку обміну інформацією між Національним банком України, комерційними банками та їх установами і органами державної податкової адміністрації України» від 14 грудня 1999 р. //Офіційний вісник України. – 1999. – № 51.

40. Постанова Правління Національного банку України № 134 «Про затвердження Інструкції про вимоги з організації охорони установ банків України» від 28 березня 2001 р.

41. Постанова Правління Національного банку України № 254 «Про затвердження Положення про організацію операційної діяльності в банках України» від 18 червня 2003 р.

42. Постанова Правління Національного банку України № 267 «Порядок передачі інформації від установ банків до органів державної податкової служби електронними засобами з питань проведення операцій відкриття, закриття рахунків; зарахування податків, повернення надмірно сплачених сум; реєстру розрахункових документів про сплату платежів до бюджету; щоденної банківської звітності за формою 412-Д» від 8 липня 1998 р.

43. Постанова Правління Національного банку України № 280 «Правила організації захисту електронних банківських документів в установах, включених до інформаційно-обчислювальної мережі Національного банку України» від 10 червня 1999 р..

44. Постанова Правління Національного банку України № 451 «Про затвердження Правил надання банками на письмову вимогу керівників відповідних спеціальних підрозділів по боротьбі з організованою злочинністю інформації і документів» від 16 листопада 2000 р.

45. Положення Національного банку України «Про відкриття та функціонування в уповноважених банках України рахунків банків-кореспондентів в іноземній валюті та в гривнях» від 26 березня 1998 р.

46. Постанова Правління Національного банку України № 540 «Про затвердження Інструкції про порядок закриття діючих анонімних валютних

рахунків фізичних осіб (резидентів і нерезидентів) або трансформації цих рахунків у інші рахунки» від 23 грудня 1998 р. //Додаток до Вісника Національного банку України. Законодавчі і нормативні акти з банківської діяльності. – 1999. – № 1.

47. Постанова Правління Національного банку України № 538 «Про затвердження Положення про порядок здійснення Національним банком України наглядових функцій щодо банків, діяльність яких пов'язана з державною таємницею» від 28 грудня 2002 р..

48. Постанова Правління Національного банку України № 367 «Положення про порядок емісії платіжних карток і здійснення операцій з їх застосуванням» від 27 серпня 2001 р.

49. Постанова Правління Національного банку України № 164 «Про схвалення Методичних рекомендацій з питань розроблення банками України програм з метою протидії легалізації (відмиванню) грошей, отриманих злочинним шляхом» від 30 квітня 2002 р..

50. Постанова Правління Національного банку України № 38 «Про затвердження Положення про застосування Національним банком України заходів впливу до комерційних банків за порушення банківського законодавства» від 4 лютого 1998 р.

51. Положення Національного банку України «Про кредитування» від 28 вересня 1995 р. № 246.

52. Положення Національного банку України «Про порядок формування і використання резерву для відшкодування можливих витрат за позиками комерційних банків» від 29 вересня 1997 р. № 323.

53. Постанова «Про затвердження нової редакції Положення про порядок формування і використання резерву для відшкодування можливих втрат за позиками комерційних банків» від 27 березня 1998 р. № 112.

54. «Положення про порядок здійснення консорціумного кредитування» НБУ від 21 лютого 1996 р. № 37.

55. Постанова Правління Національного банку України від 19 лютого 1998 р. № 56 про «Зміни до інструкції № 7 «Про безготівкові розрахунки в господарському обороті України» від 2 серпня 1996 р. № 204.

56. Постанова Правління Національного банку України № 3 «Про затвердження змін до Інструкції № 7 «Про безготівкові розрахунки в господарському обороті України» № 204 від 4 січня 2000 р. //Офіційний вісник України. – 2000. – № 4.

57. Постанова Правління Національного банку України № 573 «Про затвердження змін до Положення про застосування Національним банком України заходів впливу до комерційних банків за порушення банківського законодавства» від 30 листопада 1999 р. //Офіційний вісник України. – 2000. – № 1.

58. Адміністративне право України. – К.: Юрінком Інтер, 1999.– С.662-675.

59. *Антипенко В.Ф.* Борьба с современным терроризмом: международно-правовые подходы. – К.: Юнона – М, 2002. – 723 с.

60. *Артемьев В.* Контрразведывательная работа внутри фирмы // Справочник кадровика. – 2003. – № 3. – С.89-90.

61. Банковское дело /Под ред. О.И.Лаврушина. – М.: ТОО «ЭКОС», 1992. – 428 с.

62. Банковская энциклопедия /Под ред. С.И. Лукаш, Л.А. Малютиной. – Днепропетровск: «Кансса-Плюс«, 1994. – 250 с.

63. Банківська енциклопедія /За редакцією д.екон.н., професора Мороза А.М. – К.: Фірма «Ельтон«, 1993. – 328 с.

64. Банковская система России. Настольная книга банкира: В 3-х кн. Кн. 1 /Л.И.Абалкин и др. – М.: Дека, 1995. – 688 с.

65. *Барановський О.* Банківська система України: сьогодні і завтра // Дзеркало тижня. – 2003. – № 14. – С.8.

66. *Бершадський О.* Правова охорона службової і комерційної таємниці //Довідник кадровика. – 2003. – № 2. – С. 87-91.

67. *Біленчук П.Д., Диннік О.Г., Лютий І.О., Скороход О.В.* Банківське право: українське та європейське: Навч. посібн. /За ред. П.Д.Біленчука. – К.: Атіка, 1999. – 400 с.

68. *Бутенко О., Ермакович В.* Банки Украины: вчера, сегодня, завтра // Финансовая Украина. – 1997. – № 12. – С.18-19.

69. Великий тлумачний словник сучасної української мови /Уклад. і голов. ред. В.Т.Бусел. – К.; Ірпінь: ВТФ «Перун«, 2001. – 1440 с.

70. *Вертузаєв М.С., Голубєв В.О., Котляревський О.І., Юрченко О.М.* Безпека комп'ютерних систем. Злочинність у сфері комп'ютерної інформації та її попередження. – Запоріжжя: ПВКФ «Павел», 1998. – 316 с.

71. *Вертузаєв М.С., Ільніцький А.Ю.* Пластикові платіжні засоби в Україні і кримінологічний аспект: Навч.-практ. посібн. /За ред. проф. Я.Ю.Кондратьєва. – К.: Національна академія внутрішніх справ України, 2001. – 108 с.

72. *Гаєць В.* Майбутнє твоє, Україно //Науковий світ. – 2003. – № 1. – С. 10-11.

73. *Германчук П.* ГоловКРУ – урядовий орган, який здійснює контроль за публічними фінансами //Урядовий кур'єр. – 2003. – № 116. – С. 8.

74. Гносеология //Новейший философский словарь. – Минск: Издатель В.М.Скакун, 1998. – 950 с.

75. *Гончаров Є.С.* Існувати чи жити? – К.: «Земля і люди України». – 1992. – 29 с.

76. *Гончаренко О., Джангужин Р., Лисицин Е.* Громадський контроль і система національної безпеки //Дзеркало тижня. – 2002. – № 35. – С. 1-12.

77. *Гошко А.А., Дмитренко Г.А.* Опорная концепция формирования управленческой элиты в Украине и других восточнославянских государствах. – К.: МАУП, 2000. – 140 с.

78. *Грин Роберт*. 48 законов власти. – Пер. с англ. – М.: РИПОЛ КЛАССИК, 2002. – 576 с.

79. *Грушевський М.* Хто такі українці і чого вони хочуть. – К.; 1991. – 172 с.

80. *Гуревич И.С.* Очерки советского банковского права. – Л.: Прогресс, 1952. – С.16.

81. *Данільян О.Г., Дзьобань О.П., Панов М.І.* Національна безпека України: структура та напрямки реалізації: Навч. посібн. – Харків: Фоліо, 2002. – 285 с.

82. Демографічна криза в Україні: причини і наслідки. Із співдоповіді голови Комітету ВР України з питань національної безпеки і охорони Г.Крючкова на парламентських слуханнях 21 травня 2003 року //Голос України. – 2003. – № 101. – С. 8.

83. Держава не буде донором корумпованих хапуг: Виступ Президента України Леоніда Кучми на розширеному засіданні координаційного комітету по боротьбі з корупцією і організованою злочинністю 14 грудня 1999 р. //Урядовий кур'єр. – 1999. – 16 грудня.

84. *Дзюблюк О.В.* Організація грошово-кредитних відносин суспільства в умовах ринкового реформування економіки. – К.: Поліграфкнига, 2000. – 512 с.

85. *Дроздов Ю.И., Фартишев В.И.* Юрий Андропов и Владимир Путин. На пути к возрождению. – М.: ОЛМА-ПРЕСС, 2001. – 350 с.

86. *Дурдинець В.* Корупція – загроза безпеці України //Діло. – 1998, 27 квітня. – 4 травня.

87. Економіка України у XXI столітті: ретроперспектива і перспектива: Доповіді Асоціації вчених «Еліта економічної науки Львова» /За ред. докт. екон. наук проф. С.К.Реверчука. – Львів: ЛНУ, 2002. – 475 с.

88. Ексім, Ексім, відкрий личко! //Діло. – 1998. – 23-30 березня.

89. *Елинский В.И.* Основы методологии оперативно-розыскной деятельности: Монография. – М.: Изд-ль Шумилова И.И., 2001. – 228 с.

90. Енциклопедія Українознавства. – Львів: «Молоде життя», 1994. – Т. 1. – 400 с.

91. «Звернення Верховної Ради України до урядів і парламентів Великобританії, Канади, Кіпру, ФРН, США, Швейцарії» від 13 січня 1998 р.

92. *Зубок М.І., Ніколаєв Л.В.* Організаційно-правові основи безпеки банківської діяльності в Україні: Навч. посіб. для студ. вищ. навч. закл. Вид. 2-ге, допов. – К.: Істина, 2000. – 88 с.

93. Інформаційні технології та захист інформації: Збірник наукових праць. – Запоріжжя: Юридичний ін-т МВС України, 1998. – Вип.2. – 128 с.

94. *Кампо В.М., Нижник Н.Р., Шльоер Б.П.* Становлення нового адміністративного права України: Науково-популярний нарис /За заг.ред. В.М.Кампо. – К.: Видавничий Дім «Юридична книга», 2000. – 60 с.

95. *Карпенко В.В.* Протиріччя між виконавчою владою і місцевим самоврядуванням на регіональному рівні та механізми їх розв'язання: досвід України і Франції /Автореф. на здобуття наук. ступеня канд. наук з державного управління. – Одеса, 2000. – 24 с.

96. Керівники приходять і відходять, а кризи залишаються... з нами // Діло. – 1998, 16–23 березня.

97. Київський банківський союз: задля захисту прав та інтересів банків. Розширено склад спостережної ради КБС. //Закон і бізнес. – 2003. – № 18-19. – С. 27.

98. Указ Президента України «Про невідкладні заходи щодо посилення боротьби із злочинністю» //Голос України. – 1994, 22 липня.

99. Коваленко М. Банківські службовці: пошук працівника, працевлаштування, «вирощування» кадрів //Довідник кадровика. – 2003. – № 5. – С.55–58.

100. *Коваленко М.* Особливості трудових правовідносин в банківських установах //Довідник кадровика. – 2003. – № 4. – С.41–45.

101. *Ковальчук Т.* Якою має бути валютна політика? //Урядовий кур'єр. – 2003. – № 133. – С. 6–7.

102. *Ковалюк О.М.* Фінансовий механізм організації економіки України (проблеми теорії і практики): Монографія. – Львів: Видавничий центр Львівського національного університету імені Івана Франка, 2002. – 396 с.

103. Курс экономики: Учебник для вузов. /Под ред. Л.И.Абалкина. – М.: Финстатинформ, 1997. – 640 с.

104. *Копнин П.В.* Диалектика как логика и теория познания. – М., 1973. – 216 с.

105. *Корриган Е.* Центральный и другие банки: размышления о путях создания банковской системы рыночого типа //Экономика и жизнь. – 1990. – № 46.

106. Котовенко И.И. Безопасность кредитной деятельности банка. – К.: Демократична Україна, 1997. – 188 с.

107. Краще борги, ніж нічого... //Діло. – 1998, 23 лютого – 1 березня.

108. *Кремень В.Г., Табачник Д.В., Ткаченко В.М.* Україна: альтернативи поступу (критика історичного досвіду). – К.: «ARC-UKRAINE», 1996. – 793 с.

109. Кримінальна відповідальність за посадові злочини /В.А.Клименко, М.І.Мельник, М.І.Хавронюк. Коментар до Закону України «Про боротьбу

з корупцією»/ М.І.Мельник, Г.О.Омельченко, М.І.Хавронюк. – К.: Бліц-Інформ, 1996. – 512 с.

110. *Кулик О.* Банківська система на шляху реформи //Урядовий кур'єр. – 2003. – № 87. – С. 8.

111. *Лесечко М.Д., Малик Я.Й., Гелей С.Д., Стрельбицька Л.М. та ін.* Економічна безпека України: внутрішні та зовнішні чинники: Навч. посібн. – Львів: Видавничий центр ЛНУ імені Івана Франка, 2002. – 256 с.

112. *Лексис В.* Кредит и банки /Пер. с нем. – М.: Перспектива, 1994. – 120 с.

113. *Линда Смит и Вильям Рейпер*. Путешествие по миру мысли. Введение в историю философии. – Вид-во РПЦ, 2000. – 240 с.

114. *Лысенко Е.* Банки сотрудничают с СБУ //Деловая столица. – 2002. – № 14. – С. 16.

115. *Марконелл К.Р. Брю С.Л.* Экономика: Принципы, проблемы и политика: В 2 т.: пер. с англ. – М.: Республика, 1992. – Т.1. – 399 с.

116. *Мироненко В.* Про повернення трудових заощаджень і довіри до банків //Голос України. – 2003. – № 89. – С. 4.

117. *Млечин Л.М.* Председатели органов госбезопасности. Рассекреченные судьбы. – М.: ЗАО Изд-во Центрполиграф, 2001. Изд. 3-е, доп.– 861 с.

118. *Молчанов А.В.* Коммерческий банк современной России: теория и практика. – М.: Финансы и статистика, 1996. – 272 с.

119. *Молчанов А.В., Тавасиев А.* Банковская система России: какой ей быть? // Бизнес и банки. – 1994. – № 2. – С. 1-2.

120. *Мороз В.В.* Національна безпека – безпека людини. – К.: «Експлібрус», – 1994. – 61 с.

121. *Мочерний С.В.* Основи економічних знань: Запитання і відповіді. – К.: Феміна, 1996. – 272 с.

122. Муніципальне право України: Підручник /За ред. В.Ф. Погорілка, О.Ф. Фрицького. – К.: Юрінком. 2001. – 352 с.

123. *Нижник Н.Р., Ситник Г.П., Білоус В.Т.* Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навч. посібн. /За заг. ред. П.В.Мельника, Н.Р.Нижник. – Ірпінь, 2000. – 304 с.

124. *Омельченко Ю.* Западные эксперты пугают мир нашими политическими рисками //Сегодня. – 2002. – 12 августа. – С. 4.

125. *Осауленко О.Г.* Моделювання та управління сталим соціально-економічним розвитком: Автореф. дис. док. наук з держ. управління. – К.: Українська академія держ. управління при Президентові України, 2002. – 36 с.

126. *Осика С.Г., Коновалов В.В., Осика А.С.* Антидемпінгові, компенсаційні та спеціальні заходи. – К., 2000. – 168 с.

127. Основы экономической безопасности. (Государство, регион, предприятие, личность). /Под ред. Е.А.Олейникова. – М.: ЗАО «Бизнес-школа Интел-Синту», 1997. – 288 с.

128. Основи економічної теорії: Підручник /За ред. С.В.Мочерного. – Тернопіль: АТ «Тарнекс«, 1993. – 688 с.

129. Основи економічної теорії: політекономічний аспект: Підручник /Г.Н.Климко, В.П.Нестеренко, Л.О.Каніщенко та ін. За ред. Г.Н.Климка, В.П.Нестеренка. – К.: Вища школа, 1994. – 559 с.

130. Парламентаризм в Україні: теорія та практика. Матеріали міжнародної науково-практичної конференції. – К.: Інститут законодавства Верховної Ради України, 2001. – 657 с.

131. Пограничная ситуация //Литературная газета. – 1992. – 28 октября.

132. *Попович В.М.* Правові основи банківської справи та її захист від злочинних посягань. – К.: КШК ДПФ Дія-плюс, 1994. – 325 с.

133. *Попович В.М.* Правові основи банківської справи та її захист від злочинних посягань. – К.: Науково-видавничий центр «Правові джерела», 1995. – 325 с.

134. Проблемы обеспечения национальной безопасности в современных условиях: Материалы международной научно-практической конференции 28-29 июня 2001 года. – Минск, Институт национальной безопасности Республики Беларусь, 2001. – Т.1. – 280 с.

135. Проблемы обеспечения национальной безопасности в современных условиях: Материалы международной научно-практической конференции 28-29 июня 2001 года. – Минск, Институт национальной безопасности Республики Беларусь, 2001. – Т.2. – 293 с.

136. *Прокопенко В.І.* Трудове право України: Підручник. – Х.: Фірма «Консум«, 1998. – 480 с.

137. *Раевский К.Е.* Рыночное реформирование банковской системы в Украине: концептуальные положения //Вестник НБУ. – 1996. – № 1.

138. *Ревенко А.* Наш ВВП вперед лети, в Європі лиш зупинка...//Дзеркало тижня. – 2003. – 11 січня.

139. *Реверчук С.К., Реверчук Н.Й., Стрельбицька Л.М., Стрельбицький М.П.* Безпека малого і середнього підприємництва. – К.: ІЗМН, 1998. – 164 с.

140. *Реверчук С.К.* Малий бізнес: методологія, теорія і практика. – К: ІЗМН, 1996. – 192 с.

141. Реверчук С.К., Лазур П.Ю., Карбовник С.М. Малий і середній бізнес у зовнішній торгівлі України: основи, механізми та перспективи /За ред. докт. екон. наук, проф. С.К.Реверчука. – Львів: Тріада плюс, 2002. – 293 с.

142. Рекомендації парламентських слухань «Фінанси і банківська діяльність: сучасний стан та перспективи розвитку» Схвалено Постановою Верховної Ради України від 15 травня 2003 р. № 781-IV //Голос України. – 2003. – № 101. – С. 10.

143. *Ровинский Е.А.* Основные вопросы теории советского финансового права. – М.: Изд-во Инст. гос. и права, 1960. – С.161.

144. Русско-украинский финансово-банковский словарь /Сост. В.Н.Копорулина, И.В.Копорулина. – Х.: «Консум», 1997. – 208 с.

145. *Самофалов В.* Проблеми валютно-кредитної безпеки держави // Урядовий кур'єр. – 2001. – № 34. – С. 7.

146. *Самсоненко Л.* НБУ не збирається панькатися з відмивачами «брудних» грошей //Урядовий кур'єр. – 2003, – 7 лютого.

147. *Санцевич А.В.* Методика історичного дослідження. – АН УРСР, Ін-т історії Відп. ред. Ф.П.Шевченко – Київ: Наук. думка, 1990. Вид. 2-ге, перероб., доп. – 212 с.

148. *Святненко А.* Вибирайте банк, панове... //Дзеркало тижня. – 2003. – № 11. – С. 11.

149. *Севрук В.Т.* Банковские риски. – М.: «Дело ЛТД». – 1995. – 72 с.

150. *Семенюк В.* Десятирічний процес приватизації та його наслідки // Голос України. – 2003. – № 45-46. – С. 29-30.

151. *Сергеев В.И. и др.* Лубянка: обеспечение экономической безопасности государства: Сборник. – М.: ЗАО «Масс Информ Медиа«, 2002. – 448 с.

152. *Скакун О.Ф.* Теория государства и права: Учебник. – Харьков: Консум; Университет внутренних дел., 2000. – 704 с.

153. Сломаный меч Империи /М.Калашников. – Изд. 3-е, испр. и доп. – М.: ООО «Издательство Аспрель», 2002. – 512 с.

154. *Сохань П.* Становлення банківської системи України (1991-1994 рр.) //Банківська справа. – 1996. – № 3. – С.34–46.

155. *Станислав Цалик.* Банковская история Киева // KYIV WEEKLY. – 2003. – № 29. – С. 5.

156. *Старобижский Э.* Кадровая политика в зарубежных банках // Довідник кадровика. – 2003. – № 2. – С. 76-78.

157. *Стрельбицька Л.М.* Незаконні операції в кредитно-банківській сфері України: Монографія. – К.: Вид-во НА СБУ, 2001. – 165 с.

158. *Сурмин Ю.П., Туленков Н.В.* Методология и методы социологических исследований: Учеб. пособ. – К.: МАУП, 2000. – 304 с.

159. *Тігіпко С.* Для головного бухгалтера немає важливішого завдання, ніж служити Україні та українцям //Дзеркало тижня. – 2003. – № 13. – С.1,8.

160. Тігіпко С. Парламентські слухання: нові імпульси в діяльності банківської системи //Голос України. – 2003. – № 59. – С. 8.

161. *Туленков М.В.* Теоретико-методологічні аспекти сучасного банківського менеджменту //Додаток № 9 с.14 до журналу Персонал. – 2000. – № 4 (58). – С. 105-116.

162. Україна відрапортувала FATF, що все о'кау //Закон і бізнес. – 2002. – № 13. – С. 3.

163. Управление социалистическим производством: Организация. Экономика. Словарь. /Под ред. О.В.Козловой. – М.: Экономика, 1983. – 336 с.

164. *Фаренік С.А.* Логіка і методологія наукового дослідження: Наук.-метод. посіб. – К.: Вид-во УАДУ, 2000. – 340 с.

165. Фінансове право: Навч. посібн. для студентів юрид. вузів та факультетів. – К.: Вентурі, 1995. – 272 с.

166. Финансово-кредитный словарь: В 3-х т. – Т.2. / Гл.ред. В.Ф.Гарбузов. – М.: Финансы и статистика, 1986. – 511 с.

167. *Халфина Р.О.* Право как средство социального управления. – М.: Наука, 1988. – 256 с.

168. *Хелемский Ю.* Третье пришествие гривны //Бизнес и банки. – 1992. – № 21.

169. *Чікалін В.* Навіщо комерційним банкам зброя //Урядовий кур'єр. – 2003. – № 57. – С. 8

170. *Шаповалов А.* Зниження ризиків, або чого вчить закордонний досвід //Голос України. – 2002. – № 60. – С. 28.

171. *Швырев В.С.* Научное познание как деятельность. – М.: Политиздат, 1984. – 232 с.

172. *Шейко В.М., Кушнаренко Н.М.* Організація та методика науково-дослідницької діяльності: Підручник. – К.: Знання-Прес, 2002. – Вид. 2-ге, перероб. і доп. – 295 с.

173. Юридична енциклопедія, – К.: «Українська енциклопедія«, 1998, Т.1. – 670 с.

174. *Янковий О.* Смерть – це тільки початок. Невизначеність щодо долі майна банку «Україна» може тривати стільки ж, скільки існуватимуть активи... //Дзеркало тижня. – 2003. – № 11. – С. 9.

175. *Янчук В.* Напередодні торгівлі тільки за карбованці, або хто виграє від заборони розрахунків у ВКВ //Закон і бізнес. – 1995. – 15 лютого.

176. Як знешкодити «п'яту владу». Виступ Президента України Л.Кучми 5 серпня 1994 року //Урядовий кур'єр. – 1994. – 9 серпня.

177. *Крутовая Н.В.* В Одессе задержали мошенников, снявших через банкоматы свыше полумиллиона долларов //Факты и комментарии. – 2004 г., – № 3. – 13 января.

178. *Музика А., Азаров Д.* Про поняття злочинів у сфері комп'ютерної інформації //Право України. – 2003. – № 4. – С. 86-89.

179. *Ляпунов Ю., В.Максимов.* Ответственность за компьютерные преступления //Законность. – 1997. – № 1. – С. 9

180. *Бєляков К.І.* Злочини з використанням інформаційних технологій //Бюлетень обміну досвідом роботи: Наук.-практ. вид. МВС України. – 2001.– 131. – С. 24.

181. *Гавловський В.Д., Цимбалюк В.С.* Щодо проблем боротьби із злочинами, що вчиняються з використанням комп'ютерних технологій // Боротьба з контрабандою: проблеми та шляхи їх вирішення /Кер. авт. кол. А.І.Комарова, О.О.Крикун. – К., 1998. – Т.10. – С. 148.

182. *Лащук Є.* Інформація з обмеженим доступом як предмет злочину // Право України. – 2001. – № 3. – С. 75-78.

183. *Радутний О.Е.* Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів): Дис. канд. юрид. наук. – Харків, 2002. – С. 87.

184. Цивільний кодекс України від 16 січня 2003 р. – К.: Істина, 2003. – 368 с.

185. *Крисін В.А.* Безпека підприємницької діяльності. – М.: Фінанси і статистика, 1996.

186. *Гайкович Ю.У., Першин А.С.* Безпека електронних банківських систем. – М.: Єдина Європа, 1994.

187. Компьютерные террористы: Новейшие технологии на службе преступного мира //Энциклопедия преступлений и катастроф /Автор-составит. Т.И.Ревяко. – Минск, 1997. – С. 34.

188. *Гуцалюк М.* Протидія комп'ютерній злочинності //Право України. – 2003. – № 6. – С. 114–117.

189. *Гуцалюк М.* Координація боротьби з комп'ютерною злочинністю // Право України. – 2002. – № 5. – С. 121-126.

190. http: // www.interpol-assembly2001.com.

191. Матеріали агентства «Інтерфакс», 1995-99.

192. *Титоренко Г.А. та ін.* Комп'ютеризація банківської діяльності. – М.: Фінстатінформ, 1997.

193. *Дьомін В.С. й ін.* Автоматизовані банківські системи. – М.: Менатеп-Інформ, 1997.

194. *Аджиєв В.* Міфи про безпеку програмного забезпечення: уроки знаменитих катастроф //Відкриті системи. – 1998. – № 6.

195. *Абрамов А.В.* Нове у фінансовій індустрії: інформатизація банківських технологій. – СПб: Пітер, 1997.

196. *Кузнєцов В.Е.* Вимір фінансових ризиків //Банківські технології. – 1997. – № 9.

197. *Ліньков І.І. й ін.* Інформаційні підрозділи в комерційних структурах: як вижити і процвітати. – М.: НІТ, 1998. – 216 с.

198. *Тушнолобов І.Б., Урусов Д.П., Ярцев В.І.* Розподілені мережі. – СПб: Пітер, 1998.

199. Novell Net Ware. Керівництво користувача, 1998.

200. *Аглицький І.* Стан і перспективи інформаційного забезпечення російських банків // Банківські технології. – 1997. – № 1.

201. *Джонсон Джордж*. Розподілені системи в багатофіліальній структурі //PC Magazine/Russian Edition. 1998. – № 10.

202. *Заратуйченко О.В.* Концепції побудови і реалізації інформаційних систем у банках //СУБД. – 1996 р. – № 4.

203. *Мур Г.* Глобальний інформаційний ринок: Матеріали агентства VDM-News, моніторинг іноземної преси, 14.01.99 р.

204. *Семенов В.А.* Деякі питання інформаційно-аналітичної роботи в банку: Матеріали семінару «Практичні питання інформаційно-аналітичної роботи в комерційному банку», 24-26.03.98 р.

205. *Тарасов П.І.* Диасофт пропонує комплексні рішення для банків // Світ ПК. – 1998. – № 5.

206. Расследование преступлений в сфере экономики: Руководство для следователей. – М.: Спарк, 1999. – 415 с.

207. *Орлюк О.П.* Банківська система України. Правові засади організації. – К.: Юрінком Інтер, 2003. – 240 с.

208. *Шаваев А.Г.* Система борьбы с экономической разведкой. – М.: Издательский дом «Правовое просвещение», 2000. – 240 с.

209. *Скоморович І.Г., Кубів С.І., Вербицька Т.П. та інші.* Історія грошей та банківництва /За заг. ред. докт. екон. наук, проф. С.К.Реверчука. – Львів: ЛНУ ім.Івана Франка, 2003. – 391 с.

210. *Білоус В.Т.* Координація боротьби з економічною злочинністю: Монографія. – Ірпінь, Академія державної податкової служби України, 2002. – 449 с.

211. *Курінний Є.В.* Адміністративно-правова охорона банківської системи України та шляхи її вдосконалення: Автореф. дис. канд. юрид. наук: 12.00.07 /Українська академія внутрішніх справ. – К., 1996. – 23 с.

212. Банківська система України: теорія і практика становлення: Зб. наук. пр.: У 2 т. /Інститут економічного прогнозування НАН України; Українська академія банківської справи /А.О.Єпіфанов (голова ред. ради). – Суми: ВВП «Мрія-1» ЛТД, 1999. – Т.1. – 336 с.

213. Банківська система України: теорія і практика становлення: Зб. наук. пр.: У 2 т. /Інститут економічного прогнозування НАН України; Українська академія банківської справи /А.О.Єпіфанов. – Суми: ВВП «Мрія-1 ЛТД, 1999. – Т.2. – 660 с.

214. Збірник тез доповідей Міжнародної науково-практичної конференції «Банківська система України: проблеми становлення та перспективи розвитку» /Тернопільська академія народного господарства; Інститут банківського бізнесу /Б.С.Івасів (ред. кол.). – Тернопіль: Економічна думка, 1998. – 85 с.

215. *Костюченко О.А.* Банківське право: Банківська система. Національний банк. Комерційні банки. Розрахунки і кредитування. Ринок

цінних паперів. Національне валютне законодавство. Банківські системи зарубіжних країн. Інститут банківських таємниць: Підручник . – 3-тє вид. – К.: А.С.К., 2003. – Вид. 3-є. – 928 с.

216. *Швайка М.А.* Банківська система України: шляхи реформування і підвищення ефективності. – К.: Парламентське вид-во, 2000. – 196 с.

217. *Швайка М.А.* Яка банківська система потрібна Україні? (до концепції становлення і розвитку банківської системи України) /Верховна Рада України. Секретаріат. – К.: Вид. Верховної Ради України, 1995. – 78 с.

218. Захист інформації у банківській діяльності /М.М.Браіловський, Г.П.Лазарєв, В.О.Хорошко. – К.: ПВП «Задруга», 2003. – 158 с.

219. *Маринин В.* КГБ: структура и функции //В мире спецслужб. – 2004. – № 1. С.18-19.

Наукове видання

Стрельбицька Лілія Миколаївна
Стрельбицький Микола Павлович

ОСНОВИ БЕЗПЕКИ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ ТА БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

Монографія

Редактор *Вдовиченко Валентина Миколаївна*
Коректор *Асташева Марія Василівна*
Комп'ютерна верстка *Полончук Микола Андрійович*
Дизайн обкладинки *Ястребов Андрій Олександрович*

Підписано до друку 18.04.2004.
Формат 60 x 84 1/16. Папір офсетний. Друк офсетний. Гарнітура Newton. Умовн. друк. аркушів – 37,5. Обл.-вид. аркушів — 36.
Наклад 500 примір.
Замовлення № _____

Видавництво «Кондор»
Свідоцтво ДК № 1157 від 17.12.2002 р.
03057, м. Київ, пров. Польовий, 6,
тел./факс (044) 456-60-82, 241-83-47