ГЛАВА 6
ЗЛОЧИНИ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

6.1. Особливості кредитно-фінансової сфери як середовища скоєння злочинів

Основним об'єктом злочинної діяльності на об'єктах кредитно-фінансової сфери є грошові засоби. Привабливість грошей як об'єкту злочинів полягає в тому, що вони здатні виконувати декілька функцій. Гроші використовуються як засоби звернення, як засоби виміру вартості і як засоби накопичення.

Усі фінансові посередники мають в тій або іншій формі справу з грошима. Банк для забезпечення своєї діяльності отримує ззовні різноманітні ресурси і видає їх в трансформованому вигляді в це ж середовище. Управління своєю діяльністю банк здійснює самостійно на основі власних цілей з урахуванням дій середовища і сам же виконує власні команди управління. У діяльності як державних, так і комерційного банку проявляється його, подвійна соціально-економічна природа. З одного боку, банк є самостійним комерційним підприємством, орієнтованим на отримання прибутку від своєї діяльності. З іншого боку, банк є найважливішим кредитним інститутом і ключовим елементом інфраструктури фінансового сектора економічного механізму країни, тобто виконує роль важливого соціального інституту. Ці дві сторони як державного, так і комерційного банку знаходяться в діалектичній єдності, і їх завжди слід враховувати при аналізі поведінка банку.

Усі операції, що проводяться банками, по суті, являються купівлею або продажем грошових коштів в тій або іншій формі. Виконання операцій враховується шляхом зміни суми на різних рахунках. За рахунок маніпуляції з рівнем ліквідності банк отримує прибуток.

Якщо в звичайній торгівлі замість грошей покупець отримує товар, то в результаті банківських операцій покупець і продавець обмінюються платіжними засобами з різними засобами ліквідності.

Надаючи позики своїм клієнтам, банки, виконують роль фінансових посередників, приймаючи грошові кошти у вкладників і надаючи їх позичальникам. Ця діяльність банка приносить реальну користь усім зацікавленим сторонам. Вкладники користуються тим, що їх депозити виконують функцію засобу звернення і функцію ліквідних активів і

приносять відсотки. Позичальники користуються доступом, що відкрився їм, до великих грошових сум на досить тривалі періоди часу. Це, відбувається навіть тоді, коли більшість дрібних вкладників виявляють бажання вкласти у банк лише дуже невеликі грошові суми, причому на короткі проміжки часу. Не будь банків або яких-небудь аналогічних фінансових посередників, жодному великому підприємству взагалі не вдалося б вести ділові операції, виступаючи позичальником у дрібних інвесторів, які мають тимчасово вільні грошові кошти.

Природно, що і банки одержують прибуток з цих операцій. Вони отримують дохід, призначаючи по позиках більш високу ставку відсотка, ніж по вкладах.

Видача позик представляє собою головну операцію, яка приносить основну масу доходів банкам. Одержувач цінних паперів банком нерідко також стає джерелом доходів; він окрім усього іншого зменшує рівень ризику завдяки більшій диверсифікації банківського портфеля і приносить велику норму прибутку, чим вторинні резерви. Банк купує цінні папери, використовуючи для цього надмірні ліквідні засоби, якщо ділова, кон'юнктура недостатньо сприятлива для розширення об'ємів позикових операцій. В умовах кон'юнктури, коли криві доходів спрямовані вгору, здійснення інвестицій в довгострокові, порівняно неліквідні цінні папери і позики збільшують прибутковість.

Проте, для того, щоб оберегти себе від такого ризику, як несподівана втрата вкладів, банк повинен турбуватися про те, щоб в його розпорядженні завжди були деякі ліквідні активи, що дістали назву резервів.

До активів, що не приносять відсотки балансових остатків, відносяться: касова готівка, чеки і інші платіжні документи, гроші, що знаходяться в дорозі і на інкасуванні.

Банк повинен завжди мати готівку, оскільки згідно із законом він зобов'язаний на першу вимогу повертати готівкою гроші, покладені на ощадні і термінові депозити, наявні на розрахункових рахунках підприємств. З огляду на те, що суми готівки, кожен день, що поступають, на депозити від клієнтів банку, приблизно дорівнює сумі вилучення готівки, банк може нормально функціонувати обходячись порівняно невеликим об'ємом касової готівки в порівнянні з розмірами банківських депозитів. Банкам невигідно тримати готівкою дуже великі суми грошей із-за відносної легкості, з якою вони можуть бути вкрадені, а також тому, що ці гроші не приносять доходу у

формі відсотка. Перевищення об'єму готівки на рахунках банку свідчить про те, що або у банку, або у відношенні банку планується злочинна операція. В якості резерву комерційний банк повинен тримати суму у розмірі 2% депозитів, але ці гроші не приносять доходу, тому банки прагнуть скоротити величину резерву. Такі процеси, як зміна процентних ставок або вартості цінних паперів, також, пов'язані з певним ризиком для банку, оскільки вони можуть зробити необхідний продаж довгострокових активів у збиток, щоб вирішити будь-які проблеми, пов'язані з поточними (короткостроковими) потребами банків. Кредит може привести до безповоротних втрат банку в тих випадках, коли підприємство, що дає позику не в змозі повернути з відсотками суми, рівні отриманим ним позикам. Подібне відбувається при непродуктивному витрачанні позичених грошових коштів або, при проведенні злочинної операції. Непогашення позики в строк може бути наслідком або допущенням помилок в плануванні витрачання грошових коштів, або наслідком непередбачених або непередбачених платежів.

Банкіри добре справляються зі своїми функціями по видачі суд в тому, і тільки в тому, випадку, якщо вони безпомилково оцінюють результати передбачуваного використання. Що ж, до непередбачених платежів позичальників і подальших за ними фінансових втрат, то тут банкіри практично безсилі. Таким чином, банк здійснює свою діяльність в умовах постійного ризику.

Широке поширення, отримали різні види і форми розрахунків між економічними і фінансовими об'єктами. Одна з причин того, що безготівкові гроші стають основним засобом звернення, полягає в тому, що вони мають більше збереження, ніж готівку, яку треба зберігати і, які можуть вкрасти.

Крім того, безготівкові гроші є досить безпечним способом, здійснення платежів поштою, оскільки вони не мають внутрішньої цінності, якщо на платіжних документах не стоїть підпис. Безготівкові гроші особливо привабливі для здійснення платежів, при великих угодах.

Електронні, розрахунки за допомогою пластикових розрахункових карток привели до розрахунків «невидимими» грошима. Гроші в цьому випадку залишилися у вигляді балансових залишків. Мають місце злочинні посягання і на цю область розрахунків: підробка кредитних карток, псування касових апаратів.

Використання електронних систем прискорило процес розрахунків між банками, що знаходяться в різних містах, але в той же час привело до появи

злочинних посягань на канали зв'язку, до розшифровки кодів і зняття захисту з секретної інформації. Тобто в сферу злочинної діяльності включаються фахівці і люди - носії інтелектуального потенціалу, удосконалюються організаційні методи злочинної діяльності. Злочинність набуває організовані форми.

Комп'ютерна обробка інформації дозволяє радикально знизити витрати обігу не застосовуючи грошей. Використання обчислювальної техніки значно полегшило роботу фінансових установ, але привело до здійснення нових типів злочинів і потягу в злочинну діяльність фахівців, які раніше не брали участі в злочинних операціях, – це програмісти, оператори, інженери і техніки-електронщики.

Кредитно-фінансова сфера є привабливою для злочинного світу в силу наступних причин:

– специфічної ролі об'єктів кредитно-фінансової сфери в економічному механізмі країни;

– великої кількості грошей, що знаходяться в обороті;

– знеособленості грошей, що знаходяться в обороті;

– наявність великого числа фінансових інструментів, за допомогою яких проводяться фінансові операції;

– наявність тимчасового інтервалу між моментом виплати і моментом отримання грошей за товар, використання на цьому інтервалі фінансових документів і виконання різних операцій; використання банківських розрахунків, що відділяє за часом акт продажу від акту купівлі;

– можливості використати міжнародних банківських каналів для переказу грошей за кордон, оскільки немає гарантій, що держава не змінить податкову політику, або що мафіозні структури не перейдуть до грабунку;

– неврегульованість зовнішньоекономічної діяльності, така що велика частина валютної виручки осідає на рахунках зарубіжних банків.

Окрім об'єктивних причин, обумовлених чинниками, що роблять привабливою для злочинців кредитно-фінансову сферу, має місце причини що носять тимчасовий характер. До цих чинників можна віднести кризу в економіці, політичну нестабільність в державі, реформування економічного механізму.

Це обумовлює широкий наступ злочинців і організованих злочинних співтовариств на об'єкти кредитно-фінансової сфери, в ході якої, крім замаху загальнокримінального характеру злочинці прагнуть:

– блокувати корисну достовірну інформацію;

– спотворити інформацію**,** необхідну для ухвалення корисних рішень;

– формувати і передавати неправдиву інформацію;

– розкрити конфіденційну і закриту інформацію про рішення, що управляють, і, формувати попереджуючі дії, що знижують дієвість корисних рішень.

Окрім злочинних, мають місце легальні способи дестабілізації роботи банків. В цьому випадку для розширення сфери впливу організованих злочинних груп використовується, великий капітал, отриманий легальним шляхом.

Ставка в цьому випадку робиться на специфічні особливості функціонування кредитно-фінансової сфери і виключно на людські чинники. Криміналізації кредитно-фінансової сфери сприяє ряд причин.

По-перше, економіка і злочинність – два взаємозв'язані поняття. Чим нестабільніша економіка, чим слабкіше правове регулювання економічних злочинів, тим сильніше продуцирується злочинність.

По-друге, різке розшарування суспільства на бідних і багатих, дезорієнтація молоді, відсутність чіткої моралі сприяють розвитку злочинних посягань на особу і власність.

По-третє, в період нестабільності і росту інфляції росте прагнення до отримання миттєвої вигоди, не дивлячись на наслідки. До цього слід віднести безконтрольне вивезення сировини за кордон, ввезення відходів промислового виробництва, у тому числі і ядерних, що значною мірою посилює екологічну обстановку і кінець кінцем впливає на здоров'я і моральний клімат населення.

По-четверте, слабка присутність державності, відсутність чітких пріоритетів в зовнішній і внутрішній політиці, що у свою чергу не дозволяє розробити загальну концепцію безпеки України;

Усе це, разом узяте, створює обстановку деморалізації. У кредитно-фінансовій сфері надзвичайно велика латентність злочинів, оскільки проведення злочинних операцій дуже часто не відрізняється від проведення звичайних фінансових операцій. Виявлення їх є справою надзвичайно складною і вимагає особливої підготовки співробітників правоохоронних органів. По фактах шахрайства, розкрадання в кредитно-фінансовій сфері у багатьох випадках люди або не звертаються із заявами, або самі до пори не знають, що відносно їх скоєний злочин.

Оскільки держава, почавши економічні реформи, не створила правового регулювання цих реформ, то вакуум який таким чином виник, заповнили злочинні структури, все більше втілюючись в кредитно-фінансові інститути.

Сьогодні мало хто звертається в арбітраж або до суду для захисту своїх інтересів, з рішення економічних питань.

По-перше, ні арбітраж, ні суд не готові до масового напливу позивачів.

По-друге, справа в арбітражі може вестися роками.

По-третє, відсутній механізм втілення в життя рішень арбітражу або суду, а тому стягнення боргів може розтягнутися на роки, що особливо неприйнятно в умовах інфляції. А тому для «вибивання» боргів комерційні банки все частіше прибігають за допомогою «бригад» з кримінальних структур.

Збільшення типів фінансових операцій і різноманітність засобів звернення ведуть до відповідного збільшення типів і видів злочинів. У періоди швидкої інфляції гроші як засіб накопичення втрачають свою привабливість, незважаючи на їх високу ліквідність із-за швидкого знецінення. Це спонукає людей вкладати гроші в менш ліквідні активи, такі, як акції підприємств або інвестиційних фондів, іноземна валюта. Цим користуються злочинні елементи, які використовують прагнення людей обміняти гроші на надійніший засіб накопичення, створюють фонди, обіцяють високий дохід по акціях, збирають великі суми грошей, а потім з отриманими грошима втікають.

В умовах інфляції вітчизняна валюта швидко втрачає свою вартість і не може використовуватися як засіб накопичення, тому люди прагнуть поміняти гривні на долари або іншу іноземну валюту. При цьому росте попит на іноземну валюту, розширюються валютні операції. Цей чинник також використовують злочинні елементи для власного збагачення (фальшивомонетництво, укладення «липових» договорів).

Відомо, зміна кількості грошей, циркулюючих в економічній системі, може чинити істотну дію на реальний випуск продукту, рівень цін, зайнятість і багато інших параметрів. Оскільки контроль грошей такий важливий для економічної стабільності, аналітики і політичні діячі повинні розуміти, що проведення фінансових інтервенцій відгукнеться не лише, порушеннями фінансового механізму, але і чинить пряму дію, на політичну стабільність в державі. Є думка, що події «чорного» вівторка, грошова інтервенція з фальшивими авізо - цей тиск структури влади з боку злочинних

угрупувань. Тут спостерігається концентрація за місцем і часом зусиль з боку злочинних угрупувань і недостатня реакція на них з боку правоохоронних органів. Це обумовлено тим, що відсутній, механізм розпізнавання ознак порушень, а звідси і запізніла реакція на факти порушень. Для своєчасного припинення подібних акцій необхідно створити такий механізм. В принципі майже неможливо запобігти подібним порушенням, але завдання полягає в зведенні до мінімуму збитку від них.

У розвиненій фінансовій системі вимір кількості грошей – дуже непроста справа. Проблема полягає в тому, що в сучасній економіці різні види активів одночасно в тому або іншому ступені виконують усі три функції грошей. Тому немає чітких підстав для того, щоб провести межу власне грошима і іншими ліквідними засобами. Тим більше що часто практикується випуск ліквідних боргових зобов'язань з метою отримання грошових коштів і їх подальшого вкладення в менш ліквідні активи.

Ще єдиний аспект, що притягає злочинні елементи в кредитно-фінансову сферу, торкається використання його для переказу грошей, отриманих від продажу наркотиків і зброї. Світовий обіг грошей отриманих, в результаті наркобізнесу, настільки величезний, що тільки організована банківська система може йому ефективно протистояти. Будь-яка фінансова установа може бути використана в схемах фінансових аферистів і шахраїв для витягання незаконних грошей і їх подальшого приховання. Тому кримінальні елементи знаходять будь-яку можливість для проникнення у світову банківську систему, частиною якої є і банківська система України.

Боротися з цим явищем можна, якщо звертати увагу на усі складні нетипові великі операції, законність яких викликає сумнів. Усі дані по таких операціях повинні перевірятися, фіксуватися і бути доступними для інспекторів, бухгалтерів, ревізорів і органів правопорядку. Особлива роль у фінансових махінаціях належала і належить численним структурам, ринкової економіки, заснованим і зареєстрованим на вигаданих осіб і за підробленими документами. У більшості випадків саме під прикриттям лжепідриємств викрадалися і «відмивалися» значні засоби, які використовувалися передусім для придбання валюти.

При аналізі міжнародних валютно-кредитних відносин, фінансових посередників необхідно передусім звертати увагу на форми розрахунків. Загальноприйнятими формами міжнародних розрахунків є документарний акредитив, інкасо, банківський переказ, відкритий рахунок, аванс. Якщо,

більшість міжнародних розрахунків проводяться в готівковій формі, то це вже викликає сумнів в законності угод. Здійсненню злочинів на об'єктах фінансової сфери сприяє низька міра захищеності цих об'єктів, оскільки не реалізовуються сучасні організаційно-технічні заходи і охорону банків проводять непідготовлені люди. Видача ліцензій на право проведення банківських операцій і реєстрація банків проводяться без обстеження приміщень на технічну укріпленість. Багато хто з них розташований в непристосованих приміщеннях, не обладнаних відповідними охоронними засобами.

Актуальність боротьби з економічною злочинністю в кредитно-фінансовій сфері підтверджується ще і тим, що, за оцінками фахівців, прихований збиток від злочинних посягань в цій сфері перевищує сумарний матеріальний збиток від усіх інших корисливих правопорушень.

6.2. Аналітичні моделі зон контролю ризиків комп'ютерних злочинів у банківській діяльності

Виявлення зони підвищеного ризику в комп'ютерних злочинах дозволяє вивчення і оцінку процесів контролю у банківських інформаційних системах.

При визначенні функціональних областей банківських інформаційних систем (БІС) повинні піддаватися детальній перевірці усі компоненти системи і провести вибір з великого числа об'єктів контролю. Якщо надається можливість, то має бути проведена оцінка чинників ризику для усіх компонентів БІС. Деякі банки роблять тільки оцінку БІС в цілому, інші оцінюють кожну підсистему БІС. Кожною з них можуть бути властиві різні типи ризиків, які підлягають оцінці. Дослідник БІС повинен оцінити які з цих областей мають найбільш високий рівень ризику і тому повинні піддатися процедурі контролю.

Цілі цього процесу :

– ідентифікація об'єктів контролю з неприйнятно високою оцінкою ризику комп'ютерного злочину;

– оцінка невизначеності, яка існує відносно об'єктів контролю.

При оцінці ризиків компонентів БІС не обходжений перевіряти і контролювати параметри, які дозволяють :

1) ефективно розподілити обмежені ресурси, які є у розпорядженні перевіряючих;

2) забезпечити упевненість в тому, що необхідна інформація була отримана від управлінських структур;

3) забезпечувати основу для ефективного проведення перевірки БІС;

4) визначити вплив розглянутих об'єктів на діяльність банку в цілому.

Інформація, яка описує усі аспекти діяльності банку, використовуватиметься для визначення підсистем для оцінки ризиків і набору загроз, властивих кожній з них. Джерелами цих даних є:

– співбесіди з керівництвом банку з метою збору інформації для розробки моделей оцінки ризику БІС;

– проведення структурованих анкетних опитувань серед персоналу з метою уточнення моделей оцінки і контролю ризику БІС;

– документація про поточні перевірки БІС;

– стратегічні плани розвитку БІС;

– дані про бюджет банку;

– висновки інших перевірок;

– дані про існуючі проблеми БІС, що зібрані з інших джерел.

У зв'язку з цим необхідно проаналізувати загрози і уразливості, пов'язані з широким впровадженням інформаційних технологій банків і поява комп'ютерних систем в злочинній діяльності.

Тому при використанні БІС існує ризик знищення як деяких її власних частин, так і усієї системи, або несанкціонований доступ до її інформаційних ресурсів. Ризик нападу, протиправної дії можливо оцінити відносною оцінкою.

Тоді для БІС можуть існувати можливі загрози конфіденційності (просочування інформації, несанкціоноване використання ресурсів системи) цілісності і працездатності.

Виходячи з цього, надамо кількісну оцінку для БІС:

В - отриманий виграш для реалізації загрози;

З - витрати для реалізації загрози.

Тоді ризик можна описати так:

$$P=B/З$$

З урахуванням цього схема для оцінки комп'ютерного ризику у БІС, до складу якої входить *n* компонентів має вигляд, представлений на рис.6.1.

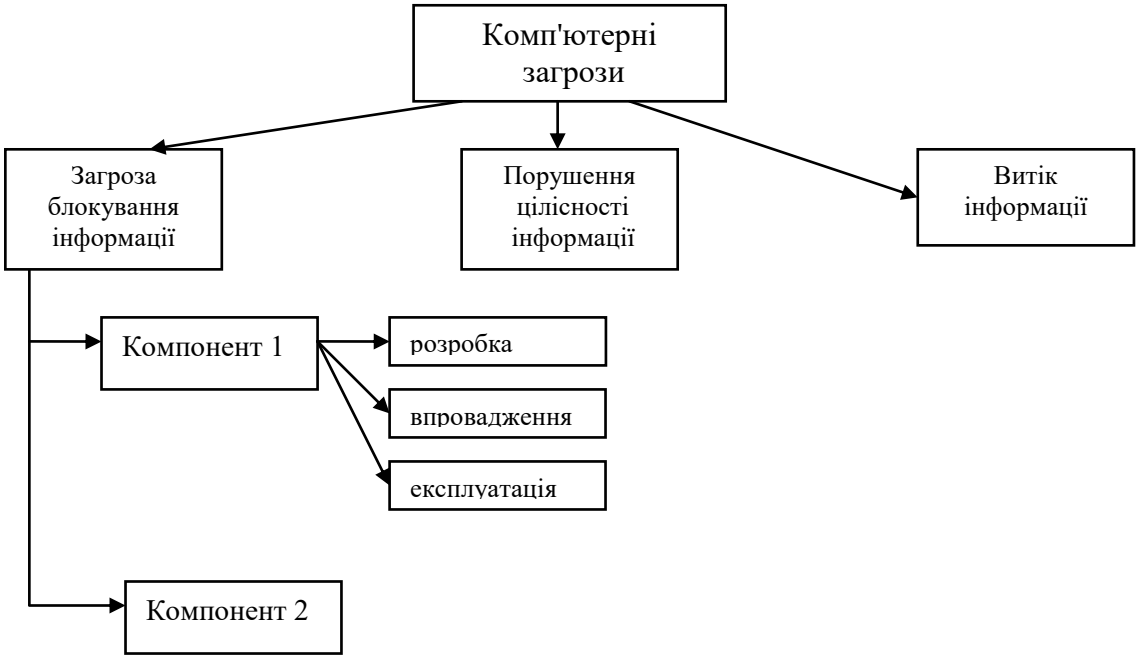

Рис.6.1. Оцінка ризику протиправних дій у БІС

Розглянемо детальніше вимоги до модуля БІС, які оцінюються. Модель оцінки ризику БІС забезпечує оцінку ризику для кожної з її підсистем, які обрані для проведення перевірки. Модуль, який підлягає перевірці, може бути окремим сегментом банку і БІС. Для його визначення немає певних правил. Проте, слід дотримуватися наступних принципів побудови моделей оцінки ризику БІС для кожного модуля або його компонента :

– модуль, який оцінюється, повинен мати чіткі, певні вхідні і початкові дані, певні процеси, що протікають в них;

– модуль має бути максимально ізольованим, тобто його оцінка не повинна зачіпати інші підсистеми.

Загальна оцінка ризику протиправної дії блокування інформації по компоненту, враховує найбільш складну і погану оцінку з усіх компонент.

Якщо ризик є допустимим, то усе залишається без змін. У іншому випадку необхідно прийняти адекватну дію із захисту інформаційної підсистеми БІС і залежних від неї ресурсів, а потім знову зробити оцінку ризику.

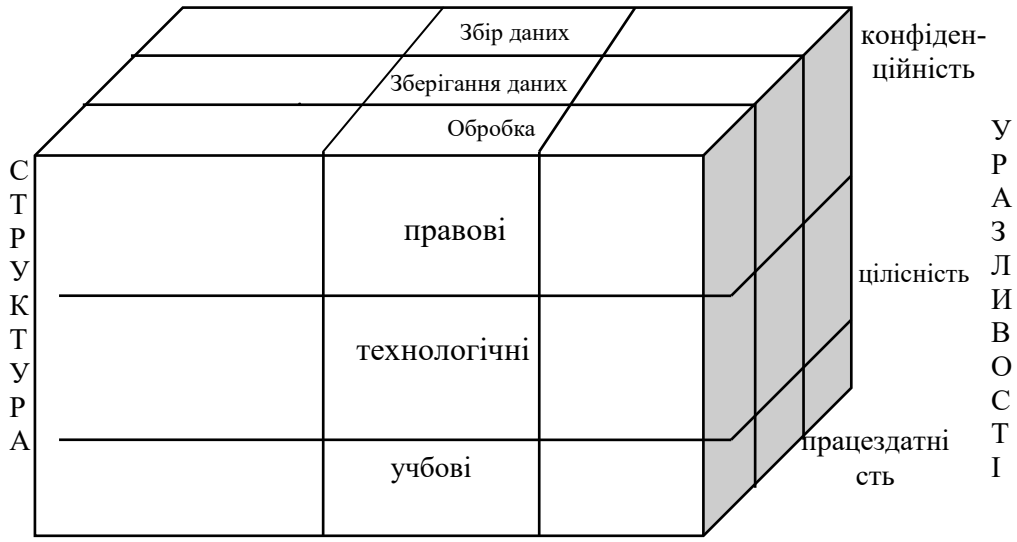

Рис. 6.2. Концептуальна модель захисту інформації від протиправних посягань у БІС

У таблиці.6.1 виконана оцінка ризику компонент БІС. Кожен модуль БІС оцінюється за вісьмома ключовими параметрами, які використовують числове ранжирування від 1(низько) до 5 (високо). Результати цих оцінок надалі перемножуються на вагові коефіцієнти, які можуть набувати значень від 1(низько) до 10(високо). Значення вагових коефіцієнтів визначаються методом експертної оцінки і залежать від багатьох чинників (архітектура, організації, профілю її діяльності, місця БІС в структурі банку, різних соціально-економічних чинників і так далі). Компоненти БІС, для яких отримані оцінки ризику, ранжуються відповідно до цих значень.

Приведемо коротке пояснення по кожному з восьми параметрів, згрупованих відповідно сумі внеску в загальну оцінку ризику.

6.2.1. Параметри оцінки негативного ефекту від можливої події.

Характер діяльності. Область, в якій болем або його підрозділ здійснює свою діяльність. Рідкісні види діяльності мають високі значення ризику.

6.2.1.1. Характер діяльності. Область, в якій банк або його підрозділ здійснює свою діяльність. Рідкісні види діяльності мають високі значення ризику.

Таблиця 6.1

Оцінка ступеня ризику

Ключові змінні	Ризикова оцінка параметрів від 1(низько) до 5 (високо)	Ваговий коефіцієнт від 1(низько) до 10(високо)

Продовження табл.6.1

1. Характер діяльності	– Діяльність, яка охоплює різні сторони життя – від 4 до 5. – Бізнес - від 2 до 3. – Локальна система - 1.	8*
2. Заходи, які застосовуються для відновлення системи у разі відмови (збою) в роботі	– Втручання не потрібне - 1. – Автоматичне відновлення - 2. – Ручне втручання - 3. – Функції БІС забезпечується установкою її попередньої версії або відмови від автоматики від 4 до 5.	5*
3. Важливість з точки зору органів управління банком	– Висока – від 4 до 5. – Середня – від 2 до 3. – Низька - 1	6*
4. Значення вкладу БІС відносно функціонування банку в цілому	Внесок БІС в доходи банку або оборот – >500.000$ – від 4 до 5. – Від 100.000$ до 500.000 $ – від 2 до 3. – < от100.000$ - 1. – Оборот > 500.000 – від 4 до 5. – Оборот від 100.000$ до 500.000$ – від 2 до 3. Оборот < 100.000$ – 1.	5*
5. Ступінь необхідного втручання обслуговуючого персоналу в роботу системи при штатному режимі роботи	Розглядаються: – Серйозне втручання – від 4 до 5. – Серйозне втручання – від 2 до 3; – Незначні корективи – 1.	8*
6. Складність	Розглядаються: об'єм обмінів, число користувачів, централізована або децентралізована БІС, число інтерфейсів. – Дуже велике – від 4 до 5. – Середнє - від 2 до 3. – Мале – 1	

Продовження табл.6.1

7. Супровід БІС в процес її роботи	– Зовнішніми розробниками – від 4 до 5. – Спеціальним персоналом – 3. – Постійно працюючим з БІС персоналом – 2. – Функції супроводу здійснюються автоматично – 1.	7*
8. Попередня оцінка виконувалася	– вказує на те, що перевірка виконувалася 5 років тому або більше – 3. – не виконувалася взагалі – 1	1*

*В даному прикладі значення довільні значення

6.2.1.2. Заходи, які застосовуються для відновлення працездатності системи у разі відмови. (збою в роботі). Оцінюються заходи, які потрібно застосовувати, щоб продовжить діяльність банку у разі порушень працездатності БІС.

Можливі варіанти продовження роботи: без втручання оператора; автоматичні операції відновлення працездатності БІС; проведення операцій відновлення працездатності БІС обслуговуючим персоналом; повернення попередньої версії математичного забезпечення БІС; повний аналіз від автоматизованої обробки інформації.

6.2.1.3. Важливість з точки зору органів управління банку. Значення цього параметра показує наскільки важливе нормальне функціонування модуля БІС з точки зору управлінських структур банку.

6.2.1.4. Значення працездатності БІС відносно функціонування банку в цілому може бути виражено в абсолютних величинах або відсотках.

6.2.2. Параметри оцінки вірогідності небажаної події у БІС.

6.2.2.1. Міра необхідного втручання обслуговуючого персоналу у функціонуванні системи при штатному режимі її роботи. Чим більша роль в організації роботи БІС відводиться людині, тим більша вірогідність появи помилок або закономірних противоправних дій. Може виникнути необхідність періодично кардинально змінювати режим роботи БІС. Крім того, подобні зміни робляться з розрахунку на довгострокову перспективу, але часто вони можуть давати короткочасний ефект, який вимагає підвищеної уваги з боку перевіряючих.

6.2.2.2. Складність. Значення цього чинника ризику відбиває збільшення чинників незаконного використання обробленої інформації, які не виявлені із-за складності структури БІС. Оцінка ступеня складності залежить від багатьох чинників: ступеня автоматизації; взаємозв'язку і взаємозалежності компонентів системи; числа компонентів або програм; функцій; проміжків часу між проведеним контролем; залежності від третіх осіб; часу обробки запитів; відповідності нормативним документів і багатьох факторів.

6.2.2.3. Супровід БІС в процесі роботи. Розглядаються наступні (поширення уразливостей) можливості супроводу системи:

- внутрішніми або зовнішніми розробками;
- спеціальним обслуговуючим персоналом;
- достатність навичок і професіоналізму співробітників, які постійно працюють і обслуговують БІС;
- закладена в структурі самої системи можливість відновлюватися.

Ризик оцінюється як мінімальний, якщо система не вимагає супроводу.

6.2.3. Оцінка невизначеності відносно результатів оцінки.

Період часу з моменту проведення останньої оцінки. Чим більший цей період часу, тим більше значення оцінки ризику. Найбільший ефект оцінки ризику дають висновки безпосередньо після його проведення.

При проведенні розширеної оцінки ризику, який поширюється на усю БІС, використовуючи ці оцінки ризику окремих її компонентів, які отримані за описаною методикою. Ці дані перемножуються на вагові коефіцієнти ділового ризику. Чинники ділового ризику (фінансового, стратегічного, операційного і юридичного) розглядаються відносно їх застосування до кожного компонента (модуля) підсистеми БІС, що підлягає оцінці.

Вагові показники чинників ділового ризику визначаються так:

1. Фінансовий ризик. Оскільки робота більшості БІС потенційно впливає на фінансову діяльність банку, рівень і вірогідність такого впливу повинні розглядатися. Якщо очікуваний ефект має непрямий вплив, відносно невеликої порівняно з іншими результатами роботи БІС. Тоді ваговий показник фінансового ризику слід прийняти рівним 0, інакше-1.

2. Стратегічний ризик. Функціонування БІС може мати прямий вплив на роботу банку в цілому аж до її припинення. Коефіцієнт встановлюється рівним 1 у разі, якщо такий вплив має місце, якщо він відсутній, то - 0.

3. Операційний ризик. Операційний ризик буде вірогідний оцінений 1

швидше чим кожен з інших чинників ризику, оскільки будь-яка БІС тісно пов'язана з повсякденною діяльністю банку, в іншому випадку - 0.

4. Відповідність законодавству і стандартам. Робота БІС залежить від того, як діяльність банку відповідає вимогам стандартів і законів і від того чи є факти противоправних дій з використанням комп'ютерної техніки і мереж.

Після проведення попередньої оцінки ризику підсистеми БІС, робиться вибір тих, з них, які піддаватимуться детальній оцінці контролю ризику. При цьому враховується оцінка його для конкретних підсистем, ресурси яких використовують контролери, керівництво банку і тому подібне.

Повний варіант оцінки і контролю ризиків застосовується у разі підвищених тренований до дійсності і безпеки інформаційних технологій соціально економічної системи. На відміну від базового варіанту, в цьому варіанті виробляється оцінка цінності ресурсів, вірогідності загроз і показників ризику. І, як правило, оптимізується склад контрзаходів за тими або іншими критеріями.

При проведенні повного аналізу ризику необхідно для конкретної БІС або її підсистеми виконати наступні дії:

1) до стандартного набору контрзаходів додати список загроз, актуальних для досліджуваної інформаційної системи;

2) визначити перелік контрзаходів, які могли б зменшити наслідки від реальних загроз;

3) по кожній загрозі визначити властивий ризик (ризик без урахування впливу контрзаходів);

4) оцінити даний ризик по кожній загрозі (як різницю властивого і залишкового ризиків);

5) оцінити вагові коефіцієнти впливів контрзаходів на загрози;

6) на основі що розглядається по загрозах і ваговим коефіцієнтам оцінити ризик, для кожного контрзаходу по кожній загрозі;

7) оцінити вартість кожного контрзаходу;

8) вирішити завдання оптимізації складу контрзаходів у БІС.

6.3. Динаміка злочинів у банківській діяльності

Ми живемо в епоху інформаційного суспільства, коли комп’ютерні та телекомунікаційні технології охопили майже всі сфери життєдіяльності суспільства і держави. Але розвиток інформаційних технологій, поширення сфери використання глобальної комп’ютерної мережі Інтернет зумовили

появу нового виду злочинності у сфері комп'ютерної інформації – комп'ютерної злочинності або кіберзлочинності.

Сьогодні жертвами осіб, які вчиняють злочини у віртуальному просторі, можуть стати не лише окремі люди чи юридичні особи, а й цілі відомства і навіть держави. Для України, як однієї з найбільших європейських держав, де у повсякденне життя стрімко входять нові комунікативні технології, зокрема, ті, що розширюють можливості реалізації товарів і послуг за допомогою мережі Інтернет, проблема кіберзлочинності не обходить жодним чином. Адже Україна входить до десятки країн із найвищим рівнем поширення цього виду криміналу, а це дитяча порнографія, шахрайства, численні порушення авторських і суміжних прав із використанням комп'ютерних систем, електронне вимагання, що в переважній більшості носять транснаціональний організований характер. З кінця 90-х років минулого століття в Україні виникла стійка тенденція до збільшення кількості злочинів у сфері високих технологій.

Нами проведений аналіз динаміки злочинів у сфері високих технологій в Україні у 2005-2013 роках за даними МВС України. Як видно з рис. 6.3, графік та лінія тренду свідчать про щорічне збільшення кількості зазначених видів злочинів.

У зв'язку з реорганізацією структури МВС України у липні 2013 року та зміною окремих форм статистичної звітності, офіційних статистичних даних щодо злочинів у сфері високих технологій за весь 2010 рік не існує. За даними Департаменту інформаційних технологій МВС України протягом 6 місяців 2013 року виявлено загалом 487 злочинів у сфері високих технологій; закінчено розслідування 309 кримінальних справ, з яких 305 направлено до суду.

Розглянемо динаміку структури злочинів у сфері високих технологій.

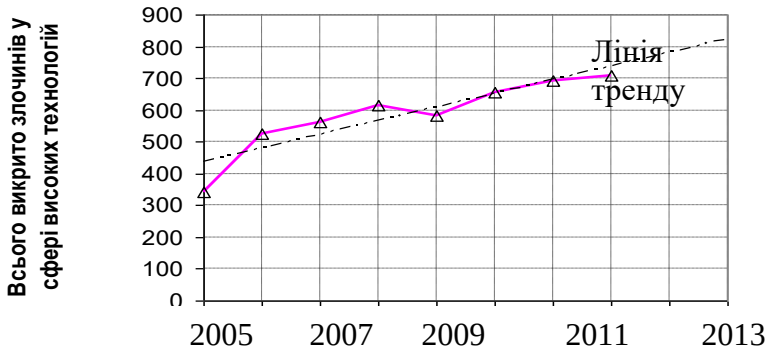

Рис.6.3. Динаміка кількості викритих злочинів у сфері високих технологій в Україні

Як видно з рис. 6.3, графік та лінія тренду свідчать про щорічне збільшення кількості викритих злочинів у сфері електронних платежів в Україні.

При аналізі рис. 6.3 можна зробити висновок, що протягом останніх п’ять років кількість викритих злочинів у сфері телекомунікацій в Україні майже не змінюється. Як видно з рис. 6.4, протягом останніх чотирьох років кількість викритих злочинів у сфері комп’ютерних та Інтернет технологій в Україні збільшилася в 2,5 рази.

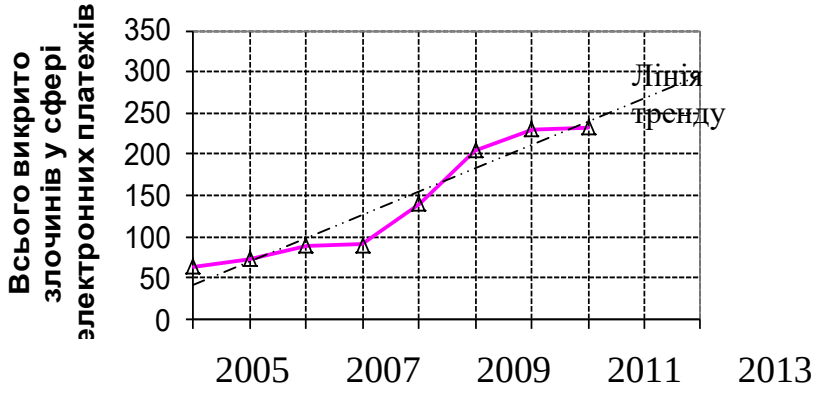

Рис. 6.4. Динаміка кількості викритих злочинів у сфері електронних платежів в Україні

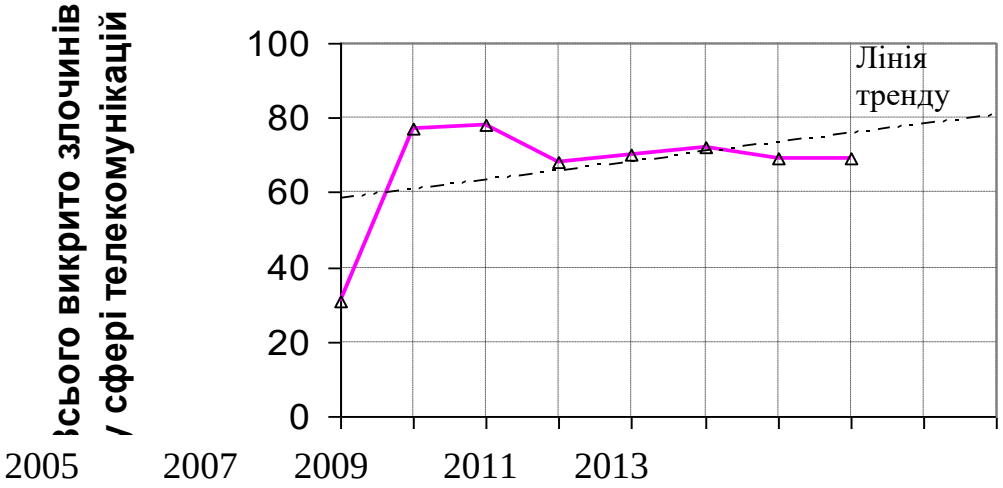

Рис. 6.5. Динаміка кількості викритих злочинів у сфері телекомунікацій в Україні

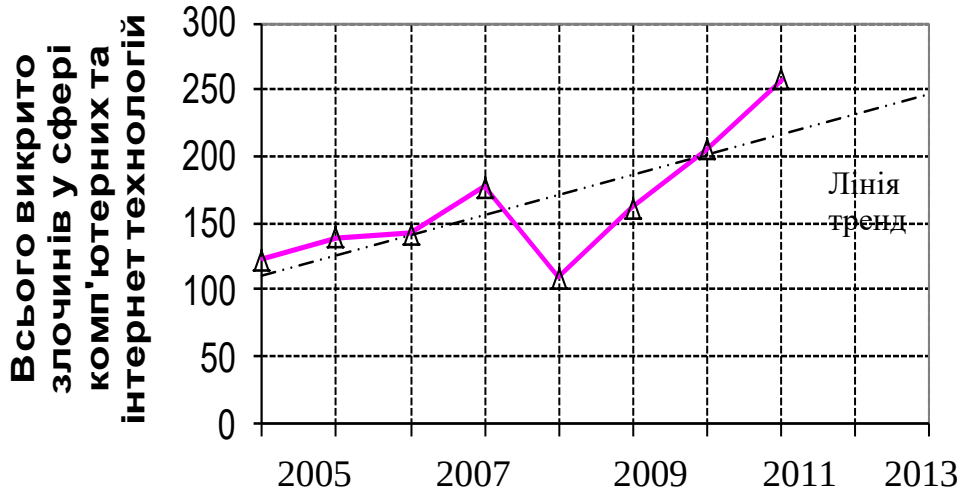

Рис. 6.6. Динаміка кількості викритих злочинів у сфері комп’ютерних та Інтернет технологій в Україні

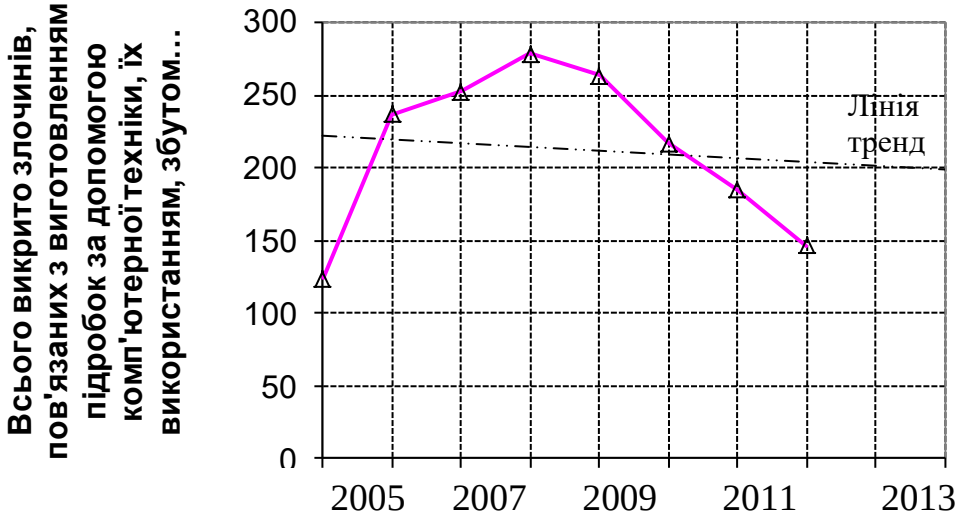

Рис. 6.7. Динаміка кількості викритих злочинів, пов’язаних з виготовленням підробок за допомогою комп’ютерної техніки, їх використанням, збутом тощо в Україні

Разом з тим, як видно з рис.6.7, протягом останніх п’яти років кількість викритих злочинів, пов’язаних з виготовленням підробок за допомогою комп’ютерної техніки, їх використанням, збутом тощо в Україні невпинно зменшується.

З аналізу даних рис.6.5 – 6.6. видно, що існує стійка тенденція до зростання кількості злочинів у сфері високих технологій, а це є важливою проблемою для правоохоронних органів, яка стала однією з першочергових і вимагає невідкладного рішення.