Дослідження/

Руслан Набок

Заступник начальника управління – начальник відділу аналізу процедур інспектування департаменту інспектування банків Національного банку України, кандидат економічних наук

Окремі питання управління операційним ризиком у банках

Розглянуто методологічні та практичні підходи до побудови системи управління операційним ризиком у банку, зокрема проаналізовано основні чинники, що можуть спричинити виникнення операційного ризику з урахуванням уроків нинішньої фінансової кризи; наведено приклади побудови системи управління операційним ризиком у банках країн – членів ЄС; виокремлено основні напрями перевірки операційного ризику банку.

ПІДХОДИ ДО ВИЗНАЧЕННЯ ПОНЯТТЯ "ОПЕРАЦІЙНИЙ РИЗИК"

Дискусія навколо побудови системи управління ризиками банку має перманентний характер [3, 4, 5]. І це природно, оскільки завдання, які ставляться перед службою ризик-менеджменту банків, відрізняються залежно від розміру банку, стратегії його розвитку, схильності до ризику, зрештою, вимог регулятора. Тому на сьогодні серед науковців і практиків немає єдиного підходу до оцінки ризиків.

Особливо актуальним є аналіз методичних основ управління операційним ризиком банку і практичних підходів до побудови системи його контролю та мінімізації. Значної уваги при цьому потребує підхід до його оцінки під час розрахунку регулятивного капіталу банку, що рекомендовано Базелем II. Відповідно до визначення, сформульованого Базельським комітетом з банківського нагляду, операційний ризик – це ризик втрат через неадекватність чи порушення (недотримання) внутрішніх процесів, збої у діяльності людей і функціонуванні системи або ризик втрат унаслідок зовнішніх подій [6]. У контексті операційного ризику виділяють юридичний ризик (legal risk) і ризик відповідності (compliance risk), що є двома аспектами однієї проблеми. Таке визначення включає правовий ризик, однак не поширюється на стратегічний і репутаційний ризики. При цьому Базельський комітет з банківського нагляду припускає, що може існувати кілька підходів до визначення терміна "операційний ризик". Тому банки для внутрішніх потреб можуть використовувати власне тлумачення операційного ризику, але за умови включення до цього поняття формулювання Базельського комітету з банківського нагляду.

У нормативно-правових актах Національного банку України операційний ризик визначено як ризик, пов'язаний із порушенням банківських правил та/або систем контролю за обробленням, проведенням операцій та за документацією, що виникає як унаслідок зовнішніх чинників, так і через помилки працівників банку [1].

ПІДСТАВИ ДЛЯ ВІДНЕСЕННЯ ОПЕРАЦІЙНОГО РИЗИКУ ДО ОКРЕМОЇ КАТЕГОРІЇ

Виділенню операційного ризику як окремої категорії ризику сприяли чинники, систематизовані в таблиці 1.

Нині не існує усталеного підходу до управління операційним ризиком, оскільки його вибір залежить від низки унікальних чинників, таких як розмір і ступінь "просунутості" (sophistication) банку, природи й складності його діяльності. Роль регулятора полягає в тому, щоб перевірити рівень управління операційним ризиком у банку, зокрема здатність банку приймати ризик і ступінь толерантності (risk appetite and tolerance) до нього.

Якісний прояв здатності приймати ризик включає відвертість і транспарентність щодо проблем контролю та подій, які призвели до втрат, котрі не слід розглядати лише як привід для покарання винних, а більшою мірою – як можливість поліпшити управління ризиками в банку.

Кількісні показники здатності приймати ризик включають неприйнятні комбінації частоти настання/серйозності, а також порогові/тригерні рівні індикаторів ризику.

У контексті управління операційним ризиком банку особливу увагу слід приділяти таким питанням:

– вплив і взаємозв'язок фінансової кризи та операційного ризику;

– культура управління ризиками;

– процедури та підходи щодо побудови системи ризик-менеджменту;

– оцінка впливу операційного ризику на капіталу банку;

– принципи використання аутсорсингу для вдосконалення процесу управління операційним ризиком.

Дослідження операційного ризику розпочалося Банком міжнародних

Таблиця 1. **Чинники впливу на розвиток операційного ризику**

Чинник	Характеристика
Технологія	Масштабне використання автоматизованих та інтегрованих технологій може трансформувати ризик від незначних помилок при ручній обробці в системні збої.
Електронна комерція	Розвиток електронної комерції супроводжується виникненням нових потенційно значущих операційних ризиків, які поки що не повністю зрозумілі.
Поглинання і злиття (об'єднання банків висуває потребу в уніфікації програмного і технічного забезпечення)	Великомасштабне злиття, поглинання, розділення й консолідація є перевіркою на життєздатність нових або щойно інтегрованих систем. Розділення (de-merger) – це операція, в ході якої одна чи кілька компаній перестають бути членами певної групи, до якої вони входили. Таким чином, за своїм значенням розділення протилежне злиттю (merger).
Роль банків, що змінюється	Перетворення банків у постачальників великої кількості послуг створює необхідність безперервно підтримувати працездатність високоефективних засобів внутрішнього контролю та резервних систем.
Методи зниження рівня ризиків	Методи зниження схильності банку до ринкового і кредитного ризиків можуть стати причиною появи інших форм ризику.
Аутсорсинг (не передаються на аутсорсинг – система управління ризиками, основні види діяльності, разові та періодичні послуги)	Аутсорсинг – це угода, згідно з якою одна фірма наймає іншу для надання певних послуг, які вона в змозі самостійно надавати або традиційно здійснювала для внутрішніх потреб. Аутсорсинг широко використовується в індустрії фінансових послуг. Передаючи частину своїх функцій зовнішнім виконавцям, банк наражається на ризик, оскільки він не зможе безпосередньо контролювати персонал компанії-постачальника послуг та/або її технічне середовище.

розрахунків зі створенням у 2003 році в межах групи з імплементації стандартів (SIG) підгрупи з дослідження питань, пов'язаних із операційним ризиком (SIGOR), та прийняттям у лютому 2003 року документа "Комплексна практика управління та нагляду за управлінським ризиком" (Sound Practices for the Management and Supervision of Operational Risk). Ця підгрупа розробляє стандарти з управління операційним ризиком та подає пропозиції до Базельського комітету з питань банківського нагляду (BCBS), який узагальнює підходи до управління операційним ризиком.

Управління операційним ризиком включає політику (стратегію) та процеси, які визначають підходи до нього, що мають передбачати такі складові, як ідентифікація, оцінка, контроль (у тому числі способи зниження рівня ризику), моніторинг. Процес оцінки операційного ризику постійно вдосконалювався – від підходів, що базуються виключно на історичних даних, до сценарного аналізу (або стрес-тесту), спрямованого на передбачення впливу операційного ризику на капітал.

На нашу думку, під час кризи не варто використовувати історичний масив даних, адже можлива значна похибка при побудові прогнозної моделі. Фінансова криза спонукала до пошуку нових шляхів управління операційним ризиком, оскільки розвинулися банківські продукти, в тому числі комплексні та інноваційні. Тому при запровадженні нових послуг банк має оцінити ризики від їх реалізації та розробити відповідні шляхи вдосконалення програмного забезпечення, процедур тощо.

Основою для управління операційним ризиком банку є стрес-тестинг, або сценарій, який передбачає наявність моделі. При управлінні операційним ризиком слід перейти від підходу, який базується на рефлексології, до проциклічного.

Протягом фінансової кризи (починаючи з 2007 року) спостерігалися збиткові події, пов'язані зі складовими операційного ризику, зокрема такі:

– обман при операціях із цінними паперами Бьонад Медофф Інвестмент Сьовісіз ЕлЕлСі (Bernard Madoff Investment Services LLC), сума збитку – 50 млрд. доларів США;

– приховані витрати/проблемні активи Веллс Кагоу енд Коу (Wells Cargo & Co), сума збитку – 8.4 млрд. доларів США;

– недозволена діяльність/управлінський облік Сосьєте Женераль Груп (Societe Generale Group), сума збитку – 7.8 млрд. доларів США;

– зовнішні злочини Феафілд Гринвич Груп (Fairfield Greenwich Group) – сума збитку 7.5 млрд. доларів США;

– викривлення звітності Петтез Груп Волвайд (Petters Group Worldwide), сума збитку – 3.0 млрд. доларів США.

Проблеми в банку виникають не через діяльність, пов'язану з ризиками (кредитний, ринковий, операційний), а через наявність та якість системи управління, ризик-менеджменту, внутрішнього контролю й стратегії. Так, проблеми, діагностовані під час пікового зростання Леман Бразерс (Lehman Brothers), виявили занадто високий рівень левериджу (20–22 до 1), неадекватні дії ради директорів, неправильні функції ризик-менеджменту, некоректну (неадекватну) стратегію зростання.

Таким чином, процес ризик-менеджменту потребує відповідного управління, принципи якого викладено в "Огляді практики ризик-менеджменту протягом наявних ринкових потрясінь" (2008 р.) та полягають у:

– ідентифікації ризику комплексно за всіма видами діяльності банку;

– послідовних практиках оцінки;

– ефективному управлінні ресурсами та ліквідністю;

– надійних процедурах оцінки та звітності щодо ризиків;

– контролі за менеджментом;

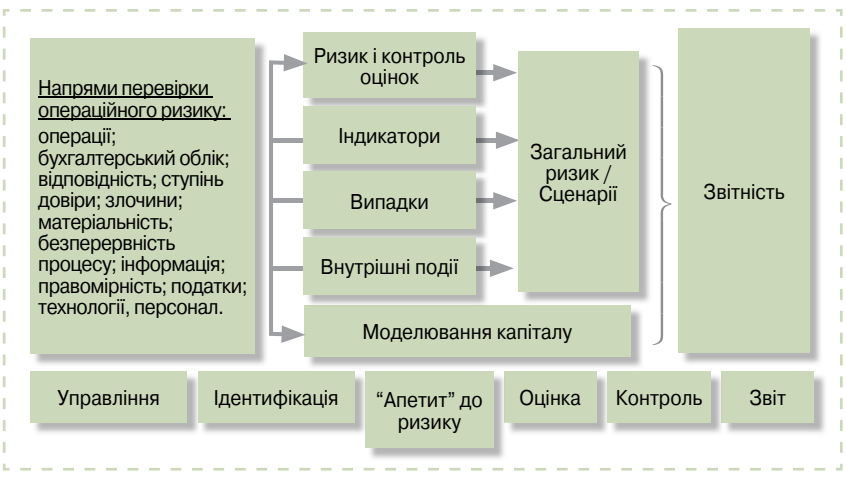
– наявності політики, процедур і лімітів;

– ідентифікації, оцінки, моніторингу ризиків та звітності за ними;

– наявності внутрішнього контролю.

У контексті операційного ризику в

Схема 1. **Елементи системи оцінки операційного ризику банку "Ейч Ес Бі Сі" (HSBC)**



системі ризик-менеджменту мають бути оцінені: персонал, процеси, технології.

ПРИКЛАДИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ОПЕРАЦІЙНИМ РИЗИКОМ У БАНКАХ ЄС

Окремо варто зупинитися на підходах, реалізованих банками країн – членів ЄС щодо управління операційним ризиком. Система управління операційним ризиком банку "Кредi С'юіс" (Credit Suisse) складається з трьох рівнів: банку, підрозділів, регіонів, на кожному з яких створено відповідні комітети і налагоджено їх взаємодію. Система нагляду за операційним ризиком Бенк Оперейшенел Ріск Оверсайт (Bank Operational Risk Oversight – BORO) передбачає вироблення узгодженої позиції комітетів різних рівнів щодо операційного ризику. У структурі банку Кредi С'юіс є департамент законодавчої відповідності Лігал Комплайенс Діпатмент (Legal Compliance Department – LCD). Процес управління операційним ризиком у банку розподілений на три блоки: дисципліна та управління ризиком; відкритість і звітність; наслідки та дії. Метою оцінки операційного ризику є визначення навантаження на капітал та визначення необхідного його рівня.

У банку "Ейч Ес Бі Сі" (HSBC) виділяються такі елементи системи оцінки операційного ризику (див. схему 1).

У банку запроваджено потрійний захист від операційного ризику: прийняття та контроль ризику (виконавчі комітети); нагляд і рекомендації (комітети з ризику); незалежний висновок (аудит).

Особливої уваги заслуговує підхід до управління операційним ризиком банку Бі Бі Ві Ей (BBVA), який полягає у використанні вдосконаленого підходу до його оцінки Ей Ем Ей (AMA). З точки зору фахівців банку будь-яка подія (операція) може впливати на результати його діяльності – приносити втрати (прямі / непрямі), або не приносити дохід (уникати його, відмовлятися від нього).

До прямих втрат відносять: прямий вплив на доходи, витрати на компенсацію, злочини, штрафи, відповідність законодавству, а також підтримка системи тощо.

До непрямих втрат відносять: неефективність (переробки, робота понад встановлені години, помилки у процесах), компенсації клієнтам, дебетування рахунків з обліку доходів, помилки цінової політики.

Відмову від доходу можуть спричинити: втрата бізнес-напрямів/клієнтів; неможливість стягування комісій; невдоволення клієнтів (як наслідок зменшення обсягу операцій, здійснюваних банком); звільнення головного персоналу; події, що впливають на репутацію банку.

З метою оцінки операційного ризику банком Бі Бі Ві Ей побудована система, яка дає змогу оцінювати як якісні чинники (компонент Ев-Роу (Ev-Ro) – система самооцінки), так і кількісні (компоненти – Транс Ва (Trans Var) (основні індикатори ризику), Ес Ай Ар Оу (SIRO) (база даних подій, що призводить до виникнення операційного ризику), Оп Віжн (OpVision) (інструмент розрахунку капіталу). При цьому використовується скоринговий метод для оцінки компонентів операційного ризику з метою переведення якісних оцінок у кількісні (інструмент Транс Ва). У банку Бі Бі Ві Ей виділено 22 якісні чинники, що можуть призводити до операційного ризику, розподілені на три категорії: людський фактор (16 чинників), технологічні (4 чинники) та зовнішні (2 чинники). Їх оцінюють за відповідним переліком питань окремо за кожним чинником.

Модель управління операційним ризиком банку Бі Бі Ві Ей передбачає розподіл повноважень (обов'язків) між центральним і лінійними підрозділами, які відповідають за операційний ризик (див. схему 2).

Банк Бі Бі Ві Ей є учасником бази даних Оу Ар Екс (ORX).

З метою управління операційним ризиком він використовує не тільки внутрішні бази даних (втрати/події), а й зовнішні, наприклад, Оу Ар Екс. На основі цих даних здійснюється аналіз сценаріїв (інструмент Ев-Роу) та контролюється середовище (інструменти Транс Ва, Ев-Роу, комітет з управління операційним ризиком і його зменшення). У банку введено окремі рахунки для обліку втрат, що виникають унаслідок здійснення операцій, які кореспондують із рахунками відповідних втрат.

Взагалі для провідних банків ЄС, США, Канади й Австралії проблема збору та отримання даних із операційного ризику (події/втрати) вирішена завдяки створенню в 2002 році бази даних Оу Ар Екс – неприбуткової асоціації зі штаб-квартирою в Цюріху. За станом на 01.10.2012 р. учасниками Оу Ар Екс є 62 банки з 18 країн. Для того, щоб стати учасником асоціації, банк сплачує разову комісію в розмірі 50.0 тис. євро та щорічну комісію за можливість отримання інформації з бази даних. За станом на 30.06.2012 р. база даних Оу Ар Екс складається з 269 430 збиткових подій на загальну суму 120.8 млрд. євро. Асоціація вирішує такі завдання: акумулює та постачає інформацію для учасників; розвиває практику управління операційним ризиком; встановлює загальні стандарти управління операційним ризиком; розвиває професійні мережі; проводить дослідження в сфері управління операційним ризиком.

Зазначимо, що центральні банки країн ЄС за допомогою рекомендацій Базельського комітету з банківського нагляду уніфікували підходи до визначення та оцінки подій, що спричиняють збитки через наявність операційного ризику.

У таблиці 2 наведено сім категорій подій, результатом яких, на думку Базельського комітету з банківського нагляду, можуть стати значні опе-

Схема 2. **Модель управління операційним ризиком банку Бі Бі Ві Ей (BBVA)**

Таблиця 2. **Події, пов'язані з операційним ризиком**

Категорія (1-й рівень деталізації)	Характеристика категорії (2-й рівень деталізації)
Внутрішнє шахрайство	Несанкціоновані дії, крадіжка чи шахрайство за участі як мінімум однієї внутрішньої сторони. Прикладами внутрішнього шахрайства можуть бути: • навмисне спотворення звітності за позиціями; • проведення недозволених операцій; • навмисне неправильне оцінювання позицій; • інсайдерські торгові операції (на власний рахунок співробітника); • умисне знищення (руйнування) активів; • крадіжка / грабіж / витрачання коштів без потреби; • хабарі / "відкати"; • фальсифікація, підробка документів; • навмисне ухилення від сплати податків.
Зовнішнє шахрайство	Розкрадання або шахрайство, здійснене третьою, зовнішньою щодо самої організації, стороною. Воно включає: • розкрадання / пограбування; • фальсифікація, підробка документів; • збиток від хакерства; • розкрадання інформації; • виписка чеків проти неінкасованих сум*.
Практика найму персоналу та гарантування безпеки праці	Ця категорія включає події, що стосуються взаємовідносин із працівниками, безпечного робочого середовища та дискримінації за різними ознаками. До них належать події, які можуть призвести до операційних збитків: • компенсаційні виплати співробітникам; • неправильне розірвання трудового договору (порушення трудового законодавства); • порушення правил охорони здоров'я і техніки безпеки; • позови у зв'язку з дискримінацією; • утиск (зокрема сексуальне домагання); • загальна відповідальність (наприклад, за нещасними випадками – "slip and fall events" тощо).
Клієнти, продукти і стандарти ведення бізнесу	Операційні ризики, що належать до цієї категорії, виникають унаслідок невиконання зобов'язань перед клієнтом, а також через характер або конструкції продукту. Це: • порушення фідуціарного боргу; • придатність послуг для клієнта / розкриття інформації (принцип "знай свого клієнта" тощо); • "накрутка" комісій за рахунками; • використання конфіденційної клієнтської інформації не за призначенням; • порушення антимонопольного законодавства; • "відмивання грошей" (легалізація доходів, одержаних незаконним шляхом); • дефекти продуктів; • перевищення лімітів ризику на одного клієнта.
Заподіяння шкоди фізичним активам	Ця категорія охоплює ризики втрат у результаті: • стихійних подій (землетруси, пожежі, повені тощо); • тероризму; • вандалізму. Крім того, включає події, результатом яких може бути не лише заподіяння шкоди фізичним активам, а й людські втрати, викликані зовнішніми причинами.
Порушення звичного режиму ведення бізнесу та відмови (негаразди, збої) систем	До цієї категорії належать такі події: • несправності (збої) апаратного та програмного забезпечення; • телекомунікаційні проблеми; • збої в енергопостачанні та наданні комунальних послуг.
Виконання операцій та управління процесом	Ця категорія охоплює ризикові події, пов'язані з обробкою операцій або управлінням процесами, взаємовідносинами з торговими контрагентами і постачальниками. Наприклад: • спотворення в процесі комунікації (передачі інформації); • помилки при введенні даних (неправильні дані, неправильне коригування за ринком тощо); • порушення термінів або зобов'язань; • неправильне функціонування моделі / системи; • помилки в бухгалтерському обліку; • порушення / недотримання зобов'язань; • відсутність або неповнота (некомплектність) юридичної документації; • неавторизований доступ до клієнтських рахунків; • суперечки з контрагентами, клієнтами, постачальниками; • аутсорсинг.

* Виписка чеків проти неінкасованих сум (check kiting) – це метод використання часу, необхідного для клірингу чеків, із метою неправомочного отримання грошових коштів без сплати відсотків за користування ними. Це одна з найпоширеніших і небезпечних форм шахрайських дій із чеками. Відомо, що в деякі схеми виписки чеків проти неінкасованих сум залучалися незабезпечені чеки на мільйони доларів, що переміщалися між різними рахунками, та несподівано перетворювались власниками у готівку перед тим, як шахраї безслідно зникали.

раційні втрати.

Наприклад, у Банку Франції з метою дослідження операційного ризику оцінюють такі події:

– операційні помилки;

– прогалини в системі внутрішнього контролю (наприклад, операції банк здійснює з некласифікованими клієнтами – німецькі банки не мають рейтингу в банку "Сосьєте Женераль");

– помилки у виборі моделі, формалізації процедур і недоліки (або недостатній рівень) формалізації процесів, що містять ризик.

Також варто відзначити важливість вдалого управління операційним ризиком у результаті процесів злиття та поглинання (M&A) банків, оскільки під час кризи спостерігається збільшення кількості подій, що призводять до збитків через недоліки в управлінні операційним ризиком. Разом із тим під час фінансових потрясінь відбувається активізація на ринку злиття та поглинання.

Пригадаймо фінансову кризу 2008 року. Саме тоді, особливо у вересні – жовтні, у банківському секторі спостерігалась активізація цих процесів. Слід відзначити такі угоди: Бі Ен Пі Паріба (BNP Paribas) поглинув Фортіс Ен Ві (Fortis NV, Бельгія та Люксембург), вартість угоди 15 млрд. євро; Веллс Фагоу (Wells Fargo) поглинув Ваковіа (Wachovia) – 11.3 млрд. євро; Ллойдс Ті Ес Бі (Lloyds TSB) поглинув Ейч Бі Оу Ес (HBOS) – 16 млрд. євро; Бенк оф Америка (Bank of America) поглинув Мерілл Лінч (Merill Lynch) – 40 млрд. євро.

Основними проблемами в контексті операційного ризику в результаті злиття/поглинання є: звільнення основного персоналу; уніфікація (інтеграція) програмного забезпечення банків, які об'єднуються. Оскільки внаслідок неузгодженості можлива втрата значного обсягу інформації, це призводить до уповільнення здійснення операцій та врешті-решт – до втрати клієнтів.

Отже, в результаті об'єднання банків має використовуватися найефективніша практика (система) побудови процесів у банківській діяльності, в тому числі ризик-менеджменту.

Щоб управляти операційним ризиком, банки виробили відповідний інструментарій щодо його мінімізації із застосуванням відповідних індикаторів визначення позиції банку щодо ризику шляхом виявлення потенційних втрат до того, як вони дійсно стануться. Зменшенню операційного ризику сприяють: страхування та передача ризику, аутсорсинг, забезпечення безперервної діяльності.

Окремим (досить поширеним) напрямом управління рівнем операційного ризику є використання банками аутсорсингу певних процесів у контексті вдосконалення процесів управління операційним ризиком. Зазначимо, що за перше півріччя 2012 року в банківському секторі та секторі фінансових послуг було укла-

Схема 3. **Система перевірки операційного ризику банку**

дено 43 угоди з ІТ аутсорсингу на загальну суму 3.8 млрд. доларів США [9]. Однак зауважимо, що на аутсорсинг не можуть бути передані такі процеси, як внутрішній аудит і менеджмент, у тому числі управління ризиками. Водночас банк, який здійснив аутсорсинг окремих процесів, не повинен відмовлятися від їх контролю з метою контролю фірм, яким передано супроводження. У зв'язку з цим регулятор повинен наглядати за процесом аутсорсингу, розробляти відповідні стандарти, вимоги до контракту тощо.

ВИСНОВКИ

Підсумовуючи викладене, зазначимо, що система управління операційним ризиком банку, а також її перевірка має бути здійснена за такими напрямами (див. схему 3).

У межах визначених напрямів перевірки операційного ризику банку доцільно сформулювати показники, за якими здійснюватиметься оцінка (наприклад, сформулювати карту бальних оцінок, запитання для отримання оцінок у розрізі критеріїв тощо). Такий підхід дасть змогу налагодити процес виявлення та оцінки операційного ризику банку й надалі відпрацювати порядок його врахування в капіталі банку. ❑

Література

1. Положення "Про організацію операційної діяльності в банках України", затверджене постановою Правління Національного банку України від 18.06.2003 р. № 254 // www.rada.gov.ua.

2. Методичні вказівки з інспектування банків "Система оцінки ризиків", затверджені постановою Правління Національного банку України від 15.03.2004 р. № 104 // www.rada.gov.ua.

3. Грибанов С. Роль ИТ-стратегии в управлении операционными рисками ритейлового банка // Системы управления бизнес-процессами. — 2008. — № 1. [Електронний ресурс]: — Режим доступу: http://journal.itmane.ru/node/29.

4. Запорожець З. Управління банківськими ризиками в контексті інформаційних технологій / Запорожець З. // Вісник Національного банку України. — 2004. — № 10. — С. 54—59.

5. Мошкалов А. Операционный риск в украинских коммерческих банках и методы его снижения / Мошкалов А.В. // Режим доступу: http://masters.donntu.edu.ua/publ2004/fem/fem_moshkalov.pdf.

6. The New Basel Capital Accord. Basel Committee on Banking Supervision. April 2003 // www.bis.org.

7. Principles for the Sound Management of Operational Risk. Basel Committee on Banking Supervision. June 2011 // www.bis.org.

8. Operational Risk — Supervisory Guidelines for the Advanced Measurement Approaches. Basel Committee on Banking Supervision. June 2011 // www.bis.org.

9. Global IT-BPO Outsourcing Deals Analysis: Quarterly Analysis // KPMG. — July, 2012.

Офіційний курс гривні щодо іноземних валют, який встановлюється Національним банком України один раз на місяць (за листопад 2012 року)*

№ п/п	Код валюти	Назва валюти		Офіційний курс	№ п/п	Код валюти	Назва валюти		Офіційний курс
1	100 BGL	100	левів (Болгарія)	529.7334	16	434 LYD	100	лівійських динарів	642.5241
2	986 BRL	100	бразильських реалів	393.7632	17	484 MXN	100	мексиканських нових песо	61.0325
3	051 AMD	10000	вірменських драмів	197.0029	18	496 MNT	10000	монгольських тугриків	57.3386
4	410 KRW	1000	вонів Республіки Корея	7.3234	19	554 NZD	100	новозеландських доларів	657.1853
5	704 VND	10000	в'єтнамських донгів	3.8336	20	586 PKR	100	пакистанських рупій	8.3443
6	981 GEL	100	грузинських ларі	481.3031	21	604 PEN	100	перуанських нових сол	307.3640
7	344 HKD	100	доларів Гонконгу	103.1339	22	642 ROL	100	румунських леїв	228.1904
8	818 EGP	100	єгипетських фунтів	130.9255	23	682 SAR	100	саудівських ріялів	213.1296
9	376 ILS	100	ізраїльських нових шекелів	204.6234	24	760 SYP	100	сирійських фунтів	11.6262
10	356 INR	1000	індійських рупій	148.0322	25	901 TWD	100	нових тайванських доларів	27.3148
11	364 IRR	1000	іранських ріалів	0.6496	26	972 TJS	100	таджицьких сомоні	167.7757
12	368 IQD	100	іракських динарів	0.6879	27	952 XOF	1000	франків КФА	15.7251
13	417 KGS	100	киргизьких сомів	16.9626	28	152 CLP	1000	чилійських песо	16.5864
14	414 KWD	100	кувейтських динарів	2842.4609	29	191 HRK	100	хорватських кун	137.5991
15	422 LBP	1000	ліванських фунтів	5.3216	30	255	100	доларів США за розр. із Індією	639.4400

* Курс встановлено з 01.11.2012 року.

Підготовлено департаментом аналізу та прогнозування грошово-кредитного ринку Національного банку України.