УДК 004.9:519.226

ДЕЯКІ АСПЕКТИ МІНІМІЗАЦІЇ ІНФОРМАЦІЙНИХ РИЗИКІВ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

Н.В. КУЗНЄЦОВА

Розглянуто основні види інформаційних ризиків, проаналізовано основні інформаційні загрози, що зустрічаються у банківській діяльності. На прикладі аналізу характеристик юридичних осіб-позичальників банку з використанням мереж Байєса було визначено причинно-наслідкові зв'язки між показниками фінансової діяльності підприємств, які збираються у фактор-листах, та виявлено ключові з них. Побудована модель мережі Байєса дозволила встановити взаємозв'язок неповернення кредитів з якістю інформаційного ресурсу, зокрема з неповнотою даних позичальника. На основі аналізу моделі було запропоновано засоби мінімізації інформаційних ризиків шляхом коректної обробки пропущених даних з урахуванням причин їх появи.

ВСТУП

Сьогодні роль і місце компанії на ринку значною мірою визначається вмінням опрацьовувати різноманітну інформацію для забезпечення своєї діяльності та захищати свою ділову, комерційну, технологічну інформацію. Особливо це стосується банківської сфери, оскільки сучасна діяльність банків переважно здійснюється в інформаційній площині (інформаційне забезпечення платіжних систем банків; інформаційно-аналітичні дослідження клієнтів, партнерів, працівників; маркетингові дослідження ринку та реклама банківських послуг; обов'язок зберігати банківську таємницю тощо), а банки є об'єктами інформаційних загроз і впливу інформаційних ризиків.

Проблемам аналізу та мінімізації ризиків присвячено роботи [1, 2], особливості інформаційних ризиків розглянуто у [3–7], але у цій роботі буде приділено увагу мінімізації інформаційних ризиків, притаманних саме банківській діяльності та пов'язаних із неповнотою інформації щодо клієнтів банку.

Мета роботи — висвітлення основних особливостей інформаційних ризиків та загроз. На прикладі аналізу діяльності банку розглянуто основні засоби та заходи, спрямовані на мінімізацію інформаційних ризиків, захист та збереження конфіденційності даних клієнтів і банківських операцій.

На основі проведеного аналізу інформаційних ризиків щодо неповноти інформації про клієнтів банку і визначення, як це може впливати на ризик неповернення позики такими клієнтами, запропонувати заходи щодо мінімізації інформаційних ризиків різної природи.

ІНФОРМАЦІЙНІ РИЗИКИ: АНАЛІЗ, ОЦІНКА, МІНІМІЗАЦІЯ

Під *інформаційними ризиками* прийнято розуміти загрозу виникнення втрат або збитків у результаті використання інформаційних технологій. Інформаційні ризики тісно пов'язані зі створенням, передачею, збереженням і використанням інформації за допомогою електронних носіїв або інших засобів зв'язку. Якщо причини виникнення інформаційного ризику знаходяться всередині підприємства, то такі ризики відносять до внутрішніх; зовнішніми інформаційними ризиками вважають ризики, які виникають внаслідок дії зовнішніх факторів.

В інформаційних взаємовідносинах підприємств наявні загрози двох видів: ті, що пов'язані з посяганнями на інформаційні ресурси, та загрози, які виникають під час формування інформаційного середовища самого підприємства.

Основними способами реалізації *інформаційних загроз* є [6, 7]:

- маніпулювання інформацією (дезінформація, викривлення інформації, запуск в інформаційне середовище неповної або неправдивої інформації);
- порушення встановленого порядку інформаційного обміну, несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів, протиправний збір і використання інформації;
- руйнування і використання чужих інформаційних ресурсів;
- інформаційний тероризм (розповсюдження вірусів, встановлення закладних пристроїв, використання засобів перехоплення інформації, незаконне використання чи порушення роботи інформаційно-телекомунікаційних систем, нав'язування фальшивої, оприлюднення компрометуючої інформації тощо).

За чинним законодавством України, інформація є об'єктом права власності, а також об'єктом володіння, використання та розпорядження. Інформаційні ризики слід розглядати і враховувати як економічні (майнові, виробничі, фінансові) [3]. Детальну класифікацію інформаційних ризиків наведено на рис. 1.

Інформаційні ризики за своїм походженням поділяються на три категорії [1]:

- ризики, пов'язані з втратою (витоком, руйнуванням, знищенням) інформації. Особливо небезпечним є ризик втрати такої інформації, як банківська таємниця, або іншої інформації з обмеженим доступом;
- ризики, пов'язані з формуванням інформаційного ресурсу (використання неповної, неправдивої інформації, відсутність необхідної інформації, дезінформація): ризики збору інформації, ризики узагальнення і класифікації, ризики обробки інформації, ризики представлення;
- ризики, пов'язані з інформаційним впливом на діяльність підприємств та банків (поширення неправдивої, негативної інформації, інформаційно-психологічний вплив на працівників, клієнтів, інформаційний тероризм).

Процес аналізу ризиків складається з декількох етапів — визначення видів ризиків, що можуть з'явитися чи уже з'явилися і впливають на діяльність того або іншого підприємства, оцінки їх впливу на діяльність підприємства та оцінки ймовірної шкоди, що може бути заподіяна внаслідок реалізації цього ризику.

Рис. 1. Класифікація інформаційних ризиків у банківській діяльності

Для управління інформаційними ризиками потрібно ідентифікувати всі можливі небезпеки, які загрожують інформаційній системі. Найчастіше під час розрахунку ризиків використовується формула [5, 7]: $AV \times EF \times ARO = ALE$, де AV (Asset Value) — вартість ресурсу; EF (Exposure Factor) — міра уразливості ресурсу до загрози; ARO (Annual Rate of Occurrence) — оцінка ймовірності реалізації загрози; ALE (Annual Lost Exposure) — підсумкові очікувані втрати від конкретної загрози за певний період часу.

Вартість ресурсів складається з вартості апаратного забезпечення, програмного забезпечення, інформації. Міра уразливості ресурсу до загрози (Exposure Factor) показує, наскільки той або інший ресурс уразливий по відношенню до даної загрози. Для якісної оцінки ризиків ця величина ранжується в діапазоні від 1 до 3, де 1 — мінімальна міра уразливості (слабка дія), 2 — середня (ресурс підлягає відновленню), 3 — максимальна (ресурс вимагає повної заміни після реалізації загрози).

Оцінка ймовірності реалізації загрози показує, наскільки ймовірна реалізація певної загрози за певний період часу (як правило, протягом року) і також ранжується за шкалою від 1 до 3 (низька, середня, висока).

Управління ризиками зводиться до зниження величин високих і середніх ризиків до значень низьких ризиків, коли стає можливим їх прийняття. Зниження величини ризику досягається за рахунок зменшення складових (AV, EF) шляхом вживання певних заходів.

Методика управління ризиками передбачає декілька способів дій. Ризик може бути:

- *прийнятий* тобто користувач згоден на ризик і пов'язані з ним витрати, тому робота інформаційної системи продовжується у звичайному режимі;
- *скасований* — мається на увазі вживання заходів щодо ліквідації джерела ризику, наприклад видалення із системи програмного забезпечення, що істотно порушує вимоги інформаційної безпеки;
- *знижений*, тобто з метою зменшення величини ризику буде вжито певні заходи;
- *переданий*, коли компенсацію потенційного збитку покладуть на страхову компанію або окремі функції будуть передані на аутсорсинг.

ІНФОРМАЦІЙНІ РИЗИКИ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

Оскільки у банках зосереджено доволі значні обсяги інформації з обмеженим доступом (банківська, комерційна таємниці, конфіденційна інформація), а на самі банки в законодавчому порядку покладено захист чужих таємниць (клієнтів банків), питання аналізу, контролю та мінімізації втрати інформації для банків є істотними. Головним в аналізі ризиків втрати інформації є виявлення способів несанкціонованого доступу до інформації банку та її найуразливіших носіїв.

Система управління інформаційними ризиками у діяльності банків має включати певні підсистеми, наприклад: підсистему захисту інформації, збору інформації та інформаційних досліджень, підсистему протидії інформаційному впливу, керуючу підсистему.

Головними завданнями підсистеми захисту інформації банку мають бути: виявлення інформації, що підлягає захисту, визначення місць зосередження та носіїв такої інформації, визначення можливих способів несанкціонованого доступу до неї, розробка і впровадження організаційних, правових, технічних, програмних, криптографічних заходів захисту інформації.

Оцінка ризиків втрати інформації у банку передбачає оцінку вартості інформаційних ресурсів, щодо яких наявний ризик втрати, й оцінку власне ризику, як імовірності реалізації певної загрози, у даному випадку пов'язаної з втратою інформації.

Вартість інформації визначається за комерційною цінністю, котра обумовлюється розміром збитків, яких можна зазнати через втрату, та перспективами вигоди, яку може отримати банк, використовуючи наявну у нього інформацію, а також — витратами, пов'язаними з виробленням, отриманням та захистом зазначеної інформації. Цінність банківської таємниці, наприклад, може бути визначена через обсяги залучених коштів від клієнтів банку, інформацію про комерційну та фінансову діяльність яких зберігає банк.

На оцінку ризику як імовірності реалізації певної загрози щодо відповідної інформації впливають такі показники, як цінність, актуальність, доступність, рівень захисту інформації.

З метою мінімізації ризику втрати інформації банківські установи мають вживати відповідні заходи, диференціюючи їх відповідно до певних загроз [1, 4]:

- формування правових умов захисту інформації, безпосередньо у банку, шляхом розробки нормативно-правових документів стосовно захисту всіх видів інформації (документованої, електронної, а також інформації, яка існує у вигляді знань працівників банку), якими мають регулюватися взаємовідносини банку з його працівниками, клієнтами тощо;
- створення системи захисту інформації, що функціонує в банківській інформаційній мережі, яка передбачатиме комплекс організаційних, технічних, криптографічних заходів і забезпечить гарантований захист від посягань на електронну інформацію банку;
- забезпечення контролю за носіями інформації, насамперед працівниками банку, стосовно дотримання ними встановленого режиму захисту інформації, своєчасне реагування на всі збої у захисті інформації;
- запровадження надійної системи документообігу (службового та спеціального діловодства), яка б виключала можливість несанкціонованого доступу до банківських документів, їх втрати, знищення чи модифікації;
- забезпечення надійної охорони банків з метою виключення можливості несанкціонованого доступу до інформації, виносу документів чи електронних носіїв інформації.

Аналіз ризиків, що можуть виникати під час формування інформаційного ресурсу банку за умов відсутності необхідного правового регулювання, свідчить, що найпоширенішими з них можуть бути: ризик відсутності необхідної банку інформації, ризик отримання та використання неповної, необ'єктивної інформації, ризик дезінформації.

Ризик відсутності інформації може виникати, коли банку терміново потрібна конкретна інформація або коли об'єкти і джерела певної інформації невідомі, що досить часто відбувається у процесі кредитної діяльності банків, у ході проведення операцій із пластиковими платіжними засобами, а також під час прийняття управлінських рішень, передусім у ході фінансового моніторингу сумнівних операцій та в процесі ідентифікації осіб, щодо

яких є підозра в легалізації («відмиванні») коштів, отриманих незаконним шляхом.

Відсутність необхідної інформації призводить до прийняття необ'єктивних рішень і, як наслідок, неефективних дій на ринку банківських послуг.

Ризик дезінформації банку стосовно умов, суб'єктів, мети взаємовідносин із банком може виникати через загострені взаємовідносини з конкурентами чи недобросовісну поведінку клієнтів.

Оцінка ризиків, пов'язаних із формуванням інформаційного ресурсу, може визначатися через ціну (вартість) певної банківської операції, щодо якої здійснюється інформаційне забезпечення, або через обсяги прибутку, які може отримати банк, прийнявши рішення на основі об'єктивної інформації. Водночас за обсягами операцій чи прибутків не можна повною мірою оцінити ризики, пов'язані з формуванням інформаційного ресурсу. За допомогою зазначених обсягів вимірюють ризик відсутності інформації. На оцінку інших ризиків суттєво впливатиме якість інформації, якою забезпечується певна операція чи рішення.

Інформаційний вплив

Інформаційний вплив — це використання спеціальних інформаційних технологій з метою формування або зміни поведінки окремих осіб чи груп осіб стосовно певних подій, об'єктів, діяльності.

Основними видами ризику інформаційного впливу для банку є:

- ризик втрати іміджу на ринку банківських послуг;
- ризик потрапляння у конфліктні ситуації з власним персоналом, клієнтами, акціонерами, державними органами тощо;
- ризик блокування роботи банку шляхом його численних перевірок.

Ризики інформаційного впливу можуть мати постійний характер, як результат певних відносин банків із різними суб'єктами, або формуватись як результат цілеспрямованої дії певних суб'єктів. В останньому випадку найхарактернішими є інформаційні атаки, коли з різних джерел одночасно або в невеликий проміжок часу в інформаційне середовище банку засилається негативна для нього інформація. Найімовірніше, що інформаційні атаки можуть здійснюватися за умов, коли банк перебуває у стані конфронтації або конкурентного суперництва чи протиборства з певними суб'єктами ринку або особами. У цьому випадку виникають вже інші види ризиків — погіршення або втрати іміджу, втрати клієнтів, зменшення обсягів операцій, понесення збитків.

Для мінімізації інформаційних ризиків впливу вдаються до таких заходів:

- періодичне поширення через різні інформаційні канали позитивної інформації про банк, оприлюднення його досягнень та активна реклама послуг;
- періодичне інформування інформаційного середовища банку, насамперед персоналу, акціонерів та клієнтів про результати його роботи;
- виховання банківського патріотизму в персоналу та акціонерів банку, пропаганда позитивного іміджу на ринку;

- проведення спеціальних інформаційних операцій стосовно зміни об'єктів інформаційного впливу, дезорієнтації суб'єктів, що вдаються до заходів впливу, контрпропаганди та попередження компрометації.

Протидія інформаційному тероризму у банківській діяльності

Під ризиком інформаційного тероризму розуміється використання різноманітних інформаційних технологій та продуктів для ураження інформаційних об'єктів (комп'ютерних мереж та систем, засобів комунікації, електронних засобів масової інформації), інформаційно-психологічного пригнічення масової та індивідуальної свідомості людей, соціальних груп на основі формування страху, високого емоційного напруження в їх поведінці.

Найчастіше в атаках інформаційного тероризму на електронні інформаційні мережі та системи, електронні бази даних застосовуються програмні засоби (комп'ютерні віруси, програмні закладки тощо), за допомогою яких терористи можуть модифікувати інформацію, блокувати її рух та доступ до неї, вилучати її. Атаки можуть здійснюватися з будь-якого місця розташування терористів, навіть з інших країн.

Під час розробки політики мінімізації цього ризику банки спочатку мають визначати, наскільки вразливими перед атаками інформаційних терористів є їх комунікаційні системи та мережі, особливо засоби, мережі та інформація, що обслуговують платіжну систему. Далі необхідно встановити, які саме ризики інформаційного тероризму найімовірніші для банку (ризик порушення роботи, руйнування інформаційних мереж і систем банку, вилучення електронної інформації, викрадення коштів, втрата іміджу банку) та можливі періоди чи обставини, за яких такі ризики найімовірніші.

Визначаються також можливі наслідки інформаційних атак терористів як з економічної точки зору, так і з погляду іміджу банку, тут формуються прогнози щодо наслідків (втрата клієнтів, звільнення провідних працівників банку, втрата інформації з обмеженим доступом, викрадення коштів із рахунків банку та його клієнтів, руйнування програмного забезпечення інформаційних систем банку).

Головне завдання полягає в тому, щоб якомога більшою мірою звузити діапазон варіантів дій терористів і відстежувати найвірогідніші та найнебезпечніші з них. Банки мають також передбачати свою поведінку в разі здійснення актів тероризму, мати уявлення про способи виживання в умовах інформаційних атак та про методи ліквідації їх наслідків.

ПОВНОТА ІНФОРМАЦІЇ У БАНКІВСЬКІЙ ДІЯЛЬНОСТІ

Одним з основних ризиків банків, пов'язаних з інформацією, є кредитний ризик. Вагомий вплив на цей ризик має внутрішній інформаційний ризик, пов'язаний з неповнотою інформації. Розглянемо взаємозв'язок кредитного (економічного) та інформаційного ризику.

Для оцінювання кредитного ризику і фактичних втрат банку часто на практиці застосовують IRB-підхід (IRB approach — internal rated based approach) — оцінки втрат внаслідок дефолтів у рамках підходу на основі внутрішніх кредитних рейтингів. Цей підхід дозволяє розробити доволі гнучкі

математичні механізми вимірювання як очікуваних, так і неочікуваних втрат, та дозволяє оцінювати індивідуальний та портфельний кредитний ризик [2].

Обсяг потенційних втрат у рамках IRB-підходу визначається як: $ECL = \sum_{i=1}^{N} PD_i \cdot CE_i \cdot LGD_i$, де основними показниками є:

- PD (probability of default — ймовірність дефолту позичальника), що набуває значення на відрізку [0,1], і чим більше значення приймає ймовірність дефолту, тим більша ймовірність того, що клієнт не поверне кредит;
- CE (credit exposure — експозиція під ризиком) — сума кредитної заборгованості;
- LGD (loss given default — покриття кредиту заставою) — покриття кредиту приймає значення від 0 (кредит повністю покритий заставою) до одиниці (кредит повністю не покритий заставою);
- N — кількість позичальників в портфелі.

Найбільш корисним показником є *ймовірність дефолту*. *Ймовірність дефолту* у час $t = 0$ визначається як ймовірність того, що клієнт перейде у стан дефолту за час $0 < t \le 1$ (року). Це означає, що лише клієнти, які ще не знаходяться у стані дефолту при $t = 0,$ отримують певну визначену для них ймовірність дефолту.

Дослідження оцінки кредитного ризику ведуться саме у напрямі розробки механізму розрахунку ймовірності дефолту, тобто процедури оцінювання ймовірності дефолту PD_i на основі певних параметрів позичальника та кредиту x_i^j: $PD_i = F(w^j, x_i^j)$, де w^j — ваги параметрів x_i^j, i — кількість позичальників, j — кількість параметрів кредиту.

Із практики діяльності банків відомо, що під час проведення кредитних операцій банки України та Росії визначають так званий ризик помилки вибору позичальника, в основу якого покладено повноту інформації про кожного конкретного позичальника. Низький ризик визначається за умов, коли наявність інформації про позичальника становить не менше 90% від обсягу даних, необхідних банку, а отримана інформація дає змогу зробити висновки про відсутність у діяльності позичальника кримінальних зв'язків, про стабільність комерційної діяльності, позитивну кредитну історію, багатопрофільну діяльність, наявність філій, добрий фінансовий стан.

Малий ризик визначається, якщо банк отримав не менш як 80% необхідної інформації про позичальника і така інформація характеризує позичальника як суб'єкта, у діяльності якого відсутні кримінальні зв'язки, підтримується стабільна комерційна діяльність на основі перспективного бізнесу, в якому беруть участь багато партнерів, а з отриманої інформації можна зробити висновок про добрий фінансовий стан та позитивну кредитну історію позичальника.

Середній ризик визначається для позичальників, щодо яких банк отримав не менш як 70% необхідної інформації. У цьому випадку інформаційні характеристики можуть вказувати на діяльність позичальника в ризиковій сфері бізнесу, на факти несвоєчасного повернення кредитів та сплати подат-

ків або відсутність досвіду роботи з кредитними коштами, велику кількість рахунків у різних банках, частина з яких є непрацюючими.

Високий ризик визначається для позичальників, щодо яких банк отримав не менше 60% необхідної йому інформації, з котрої можна зробити висновок про факти неповернення кредитів у діяльності позичальника, судові розгляди справ за позовами до позичальника, наявність кредиторських боргів, часту реорганізацію структури, велику плинність кадрів, нестійкий фінансовий стан, факти недобросовісної конкуренції з боку позичальника

Дуже високий ризик визначається за умов, коли банк отримує менше 60% необхідної йому інформації про позичальника, і отримана інформація засвідчує відсутність ознак реальної господарської діяльності, непорозуміння з правоохоронними органами та факти недбалого ставлення до виконання своїх зобов'язань, а також з отриманої інформації неможливо скласти об'єктивний висновок про фінансовий стан позичальника та можливості і перспективи його підприємницької діяльності.

Розглянемо, як повнота та достовірність отриманих банками даних впливає на оцінку кредитних ризиків.

ПРИКЛАД ОЦІНЮВАННЯ РИЗИКІВ У ПРОЦЕСІ АНАЛІЗУ КРЕДИТОСПРОМОЖНОСТІ ПОЗИЧАЛЬНИКІВ-ЮРИДИЧНИХ ОСІБ

Аналіз кредитоспроможності позичальників-юридичних осіб зазвичай здійснюється на основі затвердженого фактор-листа 55 фінансових показників, які були згруповані за такими категоріями: ліквідність, фінансовий левередж, якість активів, оборотність, прибутковість (ефективність), обслуговування боргу, розмір, структура балансу тощо.

Використання фактор-листів є стандартною загальноприйнятою методикою, при цьому зрозуміло, що не усі ці фактори є необхідними, а деякі навіть є надлишковими показниками, що дублюють або розраховуються з інших показників. Наявність в анкетах великої кількості даних призводить до випадків, коли частина факторів просто не визначається, не заповнюється підприємствами або працівниками банків через неуважність або навіть втому. У фактор-анкетах з'являються незаповнені або пропущені дані, і виявляється необхідність здійснювати аналіз повноти наданої інформації. У фактор-листах важливо розрізняти причини пропущених/незаповнених даних — неповнота заповнення пов'язана з випадковістю, недбалістю чи з неможливістю встановлення цього показника для даного підприємства. Виникає ситуація, коли з одного боку є велика кількість даних, а з іншого — ці дані не є повними або достовірними, що й викликає появу інформаційного ризику через неповноту інформації. Для мінімізації цього ризику можна скоротити кількість факторів, по яких збирається інформація, та підвищити достовірність даних — довизначити пропущені дані. Так, окремо виділяються випадки, коли пропущені дані є нормальною ситуацією (не можуть бути обчислені показники, оскільки вони в принципі не обчислюються для цих даних (галузей, клієнтів, тощо)), і випадки, коли пропуски розцінюються як найгірші випадки (спеціальне або випадкове невказування параметрів або значень, що заважає обчислити ті чи інші показники) [8, 9]. У першому

випадку пропущеним значенням присвоюється певне нейтральне значення (наприклад 0), у другому випадку — максимальне, або мінімальне значення у вибірці, і їх виділяють в окрему категорію.

Для довизначення пропущених даних було використано мережі Байєса [10, 11], які дозволили обробити і оцінити пропуски та довизначити дані там, де це було необхідно. Враховуючи, що однією з особливостей мереж Байєса є можливість з'ясувати причинно-наслідковий зв'язок між показниками, які включають у модель, побудована модель дозволила з'ясувати, які з 55 факторів є суттєвими для цієї задачі.

Для аналізу якості моделей і встановлення найкращої моделі використовуються стандартні критерії для оцінювання адекватності моделей: загальна точність; помилки I та II роду; ROC-крива та індекс GINI [11, 12].

Загальна точність моделі (CA — common accuracy) визначається як: $CA = \frac{CorrectForecast}{N}$, де $CorrectForecast$ — кількість вірно спрогнозованих випадків, а N — загальна кількість випадків. Загальна точність моделі є дещо суб'єктивною оцінкою, оскільки вона залежить від частки дефолтів у моделі, а також від порогу відсікання [12]. Для різних значень порогу точність моделі також буде приймати різні значення.

ROC-крива (Receiver Operation Characteristic — робоча характеристика приймача) показує залежність кількості вірно класифікованих позитивних прикладів від кількості невірно класифікованих негативних прикладів. Перші називають істинно позитивними, а інші — негативними множинами. При цьому припускається, що у класифікатора існує певний параметр, варіюючи який можна отримати певне розбиття на класи. Цей параметр часто називають порогом або точкою відсікання, в залежності від якого будуть отримані різні величини помилок I та II роду.

З метою перевірки статистичної значущості показників було виконано однофакторний аналіз. Цей аналіз полягає в перевірці наявності й сили зв'язку між однією залежною (показник дефолту) і незалежною змінною (фінансовий показник), що дозволяє визначити, які змінні є найбільш точними предикторами для моделі.

Однофакторний аналіз проводився у декілька кроків:

- розрахунок статистичних характеристик у ході групування на класи за принципом максимально однакової кількості спостережень у кожному класі;
- аналіз отриманих статистичних характеристик, визначення найбільш сильних предикаторів у категорії;
- перевірка отриманих закономірностей із фундаментальними знаннями з предметної області, аналіз динаміки показника *WOE* від класів;
- перегрупування на класи за допомогою зміни інтервалів з метою підвищення статистичної значущості.

Для оцінки необхідності використання всіх 55 показників було запропоновано використання моделі на основі мереж Байєса, яка дозволила б оцінити їх значущість.

В результаті проведеного аналізу було виявлено, що категорія показників ліквідності характеризується невисокою статистичною значущістю (най-

більш сильний показник — коефіцієнт загальної ліквідності); з показників фінансового левериджу для аналізу був відібраний показник — відношення боргу до капіталу; показники якості активів і ділової активності показали доволі низьку статистичну значущість та відсутність однозначних взаємозв'язків з рівнем дефолту з економічної точки зору; з показників прибутковості (ефективності) найбільш значущими виявився коефіцієнти *Prof8*. Для подальшого аналізу з показників кредитного навантаження для побудови моделі було використано показник *Debt2* (для обробки ситуацій, коли розрахувати значення цього показнику здається неможливим у випадку відсутності боргу і, як наслідок, процентних витрат, було здійснено обробку пропущених даних). Показники розміру та структури балансу характеризуються низькою статистичною значущістю і не включалися в аналіз.

В результаті були відібрані наступні 9 показників:

- Debt21 — короткостроковий борг/виручка за операційний цикл.
- Prof8 — валовий прибуток/активи.
- Debt4 — борг/(чистий прибуток + амортизація).
- Debt6 — борг/EBTDA.
- Debt2 — EDITDA/процентні витрати.
- Lev1 — валовий прибуток/чиста виручка.
- Prof1 — комбінований показник (доля необоротних активів, валовий прибуток/чиста виручка).
- Qual_str — борг/власний капітал.
- Str2 — поточні активи/активи.

Побудована мережа Байєса для оцінювання кредитоспроможності юридичних осіб представлена на рис. 2.

Для аналізу використовувались дані 299 підприємств, з них 231 — у навчальній вибірці, 78 — у перевірочній вибірці. На побудованій мережі Байєса були перевірені підприємства з перевірочної вибірки (таблиця).

Таблиця. Результати прогнозування моделі для позичальників-юридичних осіб

Факт	**Прогноз: повернення кредиту**	**Прогноз: дефолт**	**Процент точності**
Повернення кредиту	49	10	83,0%
Дефолт	5	14	74%
Загальна точність моделі			81%

Значення площі під ROC-кривою становить: $AUC = 0{,}8114$, а індекс *GINI* — $GINI = 2 * AUC - 1 = 0{,}6227$.

Аналіз даних юридичнёих осіб — позичальників кредиту показав, що відібрані 9 показників адекватно характеризують позичальника з точки зору оцінки ризику правильного вибору позичальника. З моделі видно, що найбільш важливими характеристиками для оцінювання ймовірності повернення кредиту є відносні показники Debt21 та Prof8. Використання відносних показників також є одним з варіантів обробки неповноти даних для випадків, коли дані не можуть бути обчислені з об'єктивних причин. Результати моделювання також підтвердили тісний взаємозв'язок між неповнотою да-

них, пов'язаною з навмисним незаповненням окремих показників, та ймовірністю неповернення кредиту позичальником.

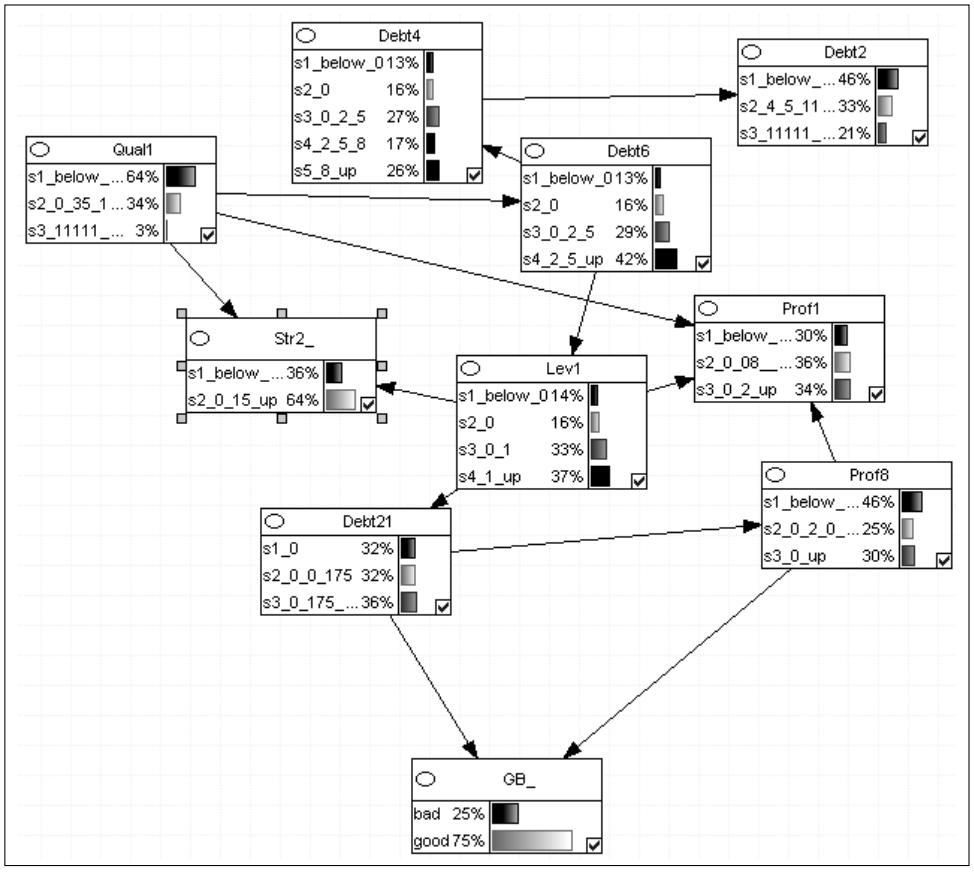

Рис. 2. Приклад структури мережі Байєса для оцінювання позичальників-юридичних осіб

Таким чином, аналізуючи інформаційний ризик, пов'язаний з неповнотою даних, за допомогою моделей мереж Байєса, можна знизити вплив цього ризику для банку, точніше оцінити загрози і можливі втрати, пов'язані з ненаданням всієї інформації позичальником, та визначити критичну інформацію, ненадання якої дозволить говорити про схильність до неповернення кредиту позичальником. Відповідна мережа Байєса у такому випадку надасть рекомендацію взагалі не видати кредит цьому підприємству, тим самим знявши повністю ймовірність реалізації цього ризику.

ВИСНОВКИ

Під час аналізу діяльності підприємства і оцінювання портфелю ризиків, що впливають на його діяльність, особливу увагу слід приділяти саме інформаційним ризикам, які проявляються як у ході проведення певної платіжної операції або транзакції, так і під час роботи програмного забезпечення всередині компанії чи технічної підтримки клієнтів, інформаційній атаці конкурентів, витоку інформації за межі компанії тощо. Засобами для мінімізації інформаційних ризиків залишаються: контроль доступу до інформації, конт-

роль і захист інформаційних систем, баз даних, тощо, від хакерських і вірусних атак, забезпечення безперебійної роботи інформаційних систем навіть в екстрених ситуаціях (наявність додаткових резервних серверів, засобів забезпечення безперебійного живлення). Стандартними засобами, що непогано працюють і у випадку інформаційних ризиків, є страхування ризиків, тобто передача ризику іншому суб'єкту (компенсацію можливих збитків покласти, скажімо, на страхову компанію) або трансформування інформаційного ризику в інші види ризику — із нижчим рівнем втрат. Банківська діяльність зазнає суттєвих впливів інформаційних ризиків, адже саме банки володіють конфіденційною інформацією про своїх клієнтів, захист персональних даних яких від спотворень, витоків та хакерських атак є однією з найважливіших задач банку. У свою чергу, в процесі збору персональної інформації про фінансовий та майновий стан клієнтів, банки також мають володіти інструментами та засобами для перевірки цих даних, їх обробки та додаткових уточнень у випадку наявності неповних та пропущених даних.

Запропонований у роботі підхід до аналізу інформаційних ризиків може бути використано для підтримки прийняття рішення про мінімізацію інформаційного ризику, пов'язаного з неповнотою даних.

ЛІТЕРАТУРА

1. *Романенко Л., Коротеєва А.* Ризики у банківській діяльності // Фінанси України. — 2003. — № 5.— С. 121–127.
2. *Кузнєцова Н.В., Бідюк П.І.* Системний підхід до аналізу кредитних ризиків з використанням мереж Байєса // Наукові вісті НТУУ «КПІ». — 2008. — № 3. — С. 11–24.
3. *Завгородний В.И.* Парадигма информационных рисков — http://www.fakit.ru/main_dsp.php?top_id=591.
4. *Петренко С., Симонов С.* Методики и технологии управления информационными риска — http://citforum.ru/security/articles/risk/.
5. *Вуколов В.* Інформаційні ризики в державному управлінні — http://archive.nbuv.gov.ua/e-journals/Patp/2010_2/10vvvrdu.pdf.
6. *Зинкевич В., Штатов Д.* Информационные риски: анализ и количественная оценка // Бухгалтерия и банки. — 2007. — № 1. — С. 50–55.
7. *Зинкевич В., Штатов Д.* Информационные риски: анализ и количественная оценка // Бухгалтерия и банки. — 2007. — № 3. — С. 48–53.
8. *Chen G., Thomas A.* Bound and Collapse Bayesian Reject Inference When Data are Missing not at Random // Proc. Conference Banff International Research Station for Mathematical Innovation and Discovery. — 2003. — 30 p.
9. *Cooman G., Zaffalon M.* Updating beliefs with incomplete observations // Artificial Intelligence. — 2004. — **159**, Iss.1–2. — P. 75–125.
10. *Згуровский М.З., Бидюк П.И., Терентьев А.Н.* Методы построения байесовских сетей на основе оценочных функций // Кибернетика и системный анализ. — 2008. — № 2. — С. 81–88.
11. *Кузнєцова Н.В, Бідюк П.І.* Порівняльний аналіз характеристик моделей оцінювання ризиків кредитування // Наукові вісті НТУУ «КПІ». — 2010. — № 1. — С. 42–53.
12. *Кузнєцова Н.В.* Інтегрований підхід до оцінювання кредитних ризиків // Тр. Одес. политехн. ун-та. — 2010. — № 1(33) — №2(34). — С. 187–192.

Надійшла 30.05.2013