Електронне наукове фахове видання "Ефективна економіка" включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)

Ефективна ЕКОНОМІКА

Дніпропетровський державний аграрно-економічний університет

№ 10, 2010 Назад Головна

УДК 330.47

М.І. Ткаченко,

кандидат економічних наук, доцент кафедри фінансів, Вінницький фінансово-економічний університет

ФОРМУВАННЯ ПРОГРАМИ КОНТРОЛЮ РИЗИКІВ ПРИ ВИКОРИСТАННІ БАНКІВСЬКИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ

У статті досліджено вплив використання електронних інформаційних систем на економічний стан банківської установи. Розглянуті можливі причини ризиків та запропонована програма заходів контролю і упередження ризиків при використанні банківських електронних інформаційних систем.

Ключові слова: *комерційний банк, економічна інформація, електронна інформаційна система, ризик, контроль.*

This article examines the impact of electronic information systems on the economic state of the banking institution. A risk control measures and prevention of risks program was proposed in case of using electronic banking systems.

Keywords: *Commerce Bank, economic information, electronic information system, risk control.*

Вступ. Діяльність всіх комерційних банків тісно пов'язана з використанням інформаційних систем, які будуються із застосуванням електронних технологій передачі, збереження, обробки, використання банківської економічної інформації. Надійне функціонування цих систем безпосередньо впливає на економічну діяльність та фінансовий стан банківської установи. В управлінні ризиками банківської діяльності разом із фінансовими ризиками необхідно враховувати ризики, які пов'язані із використанням банківських електронних інформаційних систем. Тому для управління ризиками повинна бути побудована система обліку і вивчення усіх подій, що спричиняють збитки, визначення ймовірностей їх настання для кожного реального клієнта, способи їх упередження або відшкодування збитків. Це завдання є надзвичайно важливим у сучасній банківській діяльності, його вирішення має першочергове значення.

Постановка задачі. Метою дослідження є встановлення впливу використання електронних інформаційних систем на економічний стан банківської установи та розробка рекомендацій щодо формування уніфікованої програми контролю ризиків при використанні таких систем у сучасній банківській діяльності. У дослідженні використовувались методи системного аналізу, дедукції, систематизації, класифікації.

Результати. В залежності від складності банківських інформаційних систем та характеру економічної інформації, що передається та обробляється у них, вони можуть бути згруповані таким чином:

1. **Довідкові та інформувальні системи.** До таких інформаційних систем можна віднести веб-сайти із загальною інформацією про банківську установу, реклама, новини банку, перелік послуг, ціни та тарифи на них.

2. **Електронні системи захищеної передачі інформації.** Такі системи забезпечують захищений віддалений доступ до банківських даних та пересилку економічної інформації у електронній формі, надають можливість обміну файлами, електронними повідомленнями, які містять чутливу до зовнішнього впливу або конфіденційну інформацію.

3. **Системи здійснення трансакцій.** Ці системи забезпечують клієнтам прямий доступ до банківських рахунків, надають можливість передачі електронних банківських платіжних документів (системи «Клієнт-банк»). Також такими системами забезпечується робота торговельних терміналів, банкоматів, сервісів оплати покупок в Інтернет-магазинах тощо.

Для кожної із визначених груп систем повинні проводитись процедури спостереження та дослідження якості їх роботи. Причому складність цих процедур зростає в залежності від рівня складності самої системи та чутливості інформації, що обробляється нею. Пропонуємо для банківських електронних інформаційних систем проводити можливі три рівні процедур, в залежності від визначених нами груп електронних інформаційних систем, щодо яких вони застосовуються. Наприклад, для систем першої групи застосовуватимуться процедури першого рівня складності; для систем другої групи — процедури першого та другого рівнів; а для систем третього рівня — процедури попередніх рівнів та спеціальні процедури третього рівня, якщо такі передбачені.

Дослідження ризиків, які стосуються використання банківських електронних інформаційних технологій, може здійснюватись у наступних напрямках:

1. Планування інформаційної системи, впровадження нової технології.

На цій стадії до можливих збитків може призвести: прийняття невірних рішень з розрахунку, планування і впровадження електронних технологій; вплив ціни технології на фінансовий стан банківської установи; або можливості технології, що застосовується, не відповідає потребам установи. Також причиною виникнення ризиків можуть бути огріхи в дизайні, структурі системи, що в результаті може не відповідати вимогам клієнтів до банківських послуг. Зростаюча конкуренція у галузі надання електронних банківських послуг, а також поширення різноманітних електронних платіжних систем, зокрема небанківських, повинно бути враховано при розробці та впровадженні нових технологій банківською установою.

У цьому напрямку дослідження банківських електронних інформаційних систем можуть здійснюватись наступні процедури внутрішніх спостережень за рівнями складності:

Рівень І.

Цими процедурами визначається відповідність електронних інформаційних систем складеному стратегічному плану діяльності банку і аналізу впливу специфічних ризиків на загальну банківську діяльність. Зокрема, до них належить перевірка функцій електронних каналів доставки інформації, їх відповідність стратегічному плану діяльності банку; здатність електронних засобів обробляти запланований обсяг економічної інформації.

Якщо банківська установа розширює свою діяльність за рахунок надання електронних послуг, здійснюється уточнення, чи встановлені порядки і процедури оформлення і ведення рахунків клієнтів відповідають новим видам діяльності.

Керівництво повинно бути впевненим, що персонал, призначений для розробки і впровадження електронних банківських послуг є кваліфікованим і досвідченим; функціональні обов'язки цих працівників чітко визначені і розподілені; персонал забезпечений всіма необхідними ресурсами для виконання поставлених завдань. Кожна електронна система перевіряється на відповідність встановленим стандартам функціонування. Для цього проводиться:

- тест об'ємів збереження інформації (для того, щоб переконатись в достатній ємності системи);
- тест пошуку і відображення потрібної інформації (для коректного її відображення);
- перевірка гнучкості або стрес-тест в умовах, які наближені до реальних.

Встановлення адекватності кваліфікації персоналу і його навчання стосовно використання електронних банківських систем, включаючи осіб, відповідальних за банківські продукти та послуги, інформаційні системи, перевірку і нагляд, узгоджуються юридичні питання тощо.

Рівень II.

Процедури цього рівня визначають, чи керівництво банку та відповідальні підрозділи отримують необхідну інформацію про функціонування кожної впровадженої електронної системи та здійснюють її аналіз, зокрема:

- встановлюється, чи враховуються різні аспекти функціонування електронних банківських систем, включаючи аналіз критичних випадків, збоїв;
- перевіряється, чи керівництво підрозділу або всього банку отримує звіти з якості функціонування систем для прийняття управлінських рішень.

Для кожної електронної системи, яка співпрацює з головною операційною системою банку, базами даних, визначається їх сумісність і захищеність.

Перевіряється точність та інтелектуальність програмного забезпечення з фінансового планування, розрахунків тощо, яке доступне через банківські електронні системи.

Визначається, чи встановлена система дублювання для користувачів-працівників банку, на випадок, коли системи електронних послуг банку не працюють тривалий період часу:

- необхідно переконатись про наявність необхідних інструкцій щодо використання системи дублювання;
- перевірити наявність розроблених процедур повідомлення працівників банку і клієнтів у разі виникнення технічних проблем.

Перевіряється наявність розподілу фізичного доступу до комп'ютерного обладнання, програмного забезпечення, комунікаційного обладнання і ліній комунікацій з чітко визначеними особами персоналу в залежності від їх функцій і посад в банківській установі.

Рівень III.

Процедур цього рівня при плануванні і впровадженні банківських електронних інформаційних систем не предбачено.

2. Внутрішньобанківський операційний порядок і процедури.

Організація діяльності банківської установи повинна бути пристосована до умов використання електронних засобів, тому некомпетентність керівництва, чи недосконаліть технологій які використовуються у банківській діяльності можуть вплинути на економічний стан установи. Також, вже існуюча організація діяльності може недостатньо захищати конфіденційну електронну банківську інформацію. Існуючі порядки і процедури можуть не враховувати швидкість здійснення трансакцій і розширену географію досяжності електронних каналів, якими передається банківська економічна інформація.

У цьому напрямку дослідження інформаційних систем банку здійснюються наступні перевірки:

Рівень I.

Ціль спостереження операційних порядків і процедур полягає у визначенні їх придатності в умовах використання електронних каналів передачі інформації. Визначається, чи застосовувані порядки організації праці персоналу відповідають вимогам впровадження нових банківських продуктів та послуг, як впливають електронні технології на канали передачі банківської інформації.

Банк повинен мати належну програму безпеки електронного банкінгу, що включає такі елементи:

- контроль доступу та захисту конфіденційної інформації клієнтів;
- методи визначення права запиту кожного учасника електронних систем передачі банківських даних щодо інформації про стан рахунків, можливостей зміни цього стану (безпосередньої або шляхом доручення);
- визначається, яка інформація може бути доступною для третіх осіб;
- визначається можливість доступу або спостереження (моніторингу) третіми особами електронних трансмісій (передач даних) між банком та його клієнтами.

Рівень II.

Визначається спроможність вдосконалення порядків і процедур відповідно до застосування електронних технологій забезпечення доступу і зміни конфіденційної інформації клієнтів банку.

- яку інформацію та яким чином дозволено передавати третім особам;
- чи порядок використання конфіденційної банківської інформації є частиною контрактів і угод з найманими банком третіми особами.

Також визначається, чи керівництво встановлює порядки і процедури, які контролюють будь-які можливості доступу та моніторингу електронних трансмісій між банком і клієнтом третіми особами, для цього повинні бути включені чіткі інструкції у вигляді частини контракту або угоди, що зумовлюють відносини замовника-банку та стороннього виконавця.

Рівень III.

Визначається наявність в процедурах обов'язкового засвідчення авторизації з боку клієнта для кожного списання з рахунку або переказу грошей:

- яким чином банк перевіряє легітимність кожного платежу;
- чи банком розроблені конкретні інструкції з додання чи виключення доручення на платіж клієнтом.

Далі встановлюється наявність процедур контролю наявності коштів клієнта з кожної точки доступу до рахунку. Підтверджується наявність захисту відстеження і запобігання подвійних трансакцій в кожній електронній системі. Перевіряється якість проведення навчання клієнтів відносно захисту і безпеки при використанні електронних банківських систем.

Періодично за встановленим графіком перевіряється весь спектр трансакційних банківських можливостей (в т. ч. кореспондентські і консолідовані рахунки), операційні порядки і процедури здійснення трансакцій та відповідність вимогам захисту та безпеки банківської інформації.

Встановлюється наявність затверджених порядків і процедур щодо наступних дій клієнтів:

- перевід коштів (чи може клієнт ініціювати трансакції у межах СЕП і інших платіжних систем, якщо так, то чи передбачені в цьому разі необхідні процедури безпеки проведення платіжних операцій);
- обмеження сум по часу проведення трансакцій (наприклад, визначена сума грошей в день);
- визначені стандарти мінімального кредитування;
- інструкції з управління рахунком;

Для систем, що дозволяють доступ до кредитних ліній, визначається їх контрольованість банком. Контролюється також наявність встановлених порядків і процедур при операціях з іноземною валютою, якщо на такі дії банк має відповідний дозвіл.

Перевіряється існування затверджених графіків чергувань персоналу, з огляду на застосування електронних технологій у банківській діяльності.

3. Моніторинг внутрішньої банківської діяльності.

Дані проведених спостережень, фінансова та інша звітність банку потенційно можуть мати виток в електронних системах, тому у цьому напрямку повинні проводитись процедури перевірки наступного характеру:

Рівень І.

Процедурами цього рівня визначається, чи потрапляє в поле зору програм внутрішнього та зовнішнього банківського аудиту банківська діяльність із використанням електронних інформаційних систем.

Для цього перевіряється укомплектованість відділу внутрішнього аудиту кваліфікованим персоналом та обладнанням в умовах використання електронних інформаційних систем у банківській установі.

Рівень ІІ.

Контролюється, чи кожна впроваджена система підлягає перевіркам.

Рівень ІІІ.

Повинні здійснюватись процедури спостереження за електронною трансакційною діяльністю (від моменту ініціації до завершення) всіх банківських систем обслуговування.

4. Правові питання.

За сучасних умов ведення господарювання зберігається юридична невизначеність застосування електронних контрактів, угод, підписів; питання захисту приватної інформації клієнтів; невизначеність правових заходів за кримінальним і цивільним законодавством стосовно неправомірного використання економічної інформації; відсутня чітка регуляція міжнародної банківської діяльності із застосуванням міжнародних платіжних систем (зокрема небанківських). Також залишається невизначеним поняття електронних грошей і застосування їх банками. Невизначеною є юридична сила електронних банківських документів. Тому така нечіткість юридичного підґрунтя діяльності банківських установ із використанням електронних та комунікаційних засобів може бути причиною виникнення ризикових ситуацій та можливих збитків.

Зокрема, здійснюються спостереження у наступних напрямках:

Рівень І.

Спостерігається, чи управлінням банку визначено інструкції проведення рекламних повідомлень і акцій. Перевіряється наявність юридичної інформації у електронній рекламі банківських послуг.

Рівень ІІ.

Визначається правове забезпечення клієнтських угод, що складаються; тобто чи передбачені права і відповідальності кожної сторони. За банком повинно зберігатись право спостереження, зберігання і отримання електронних потоків інформації (повідомлень і даних) між банком та його клієнтами.

Керівництвом банку повинна бути визначена відповідальність сторін і статус електронних підписів і сертифікатів у вирішенні правових питань.

Контролюється, чи зовнішні угоди з постачальниками обладнання або підрядниками відповідають вимогам захисту клієнтів банку.

Рівень ІІІ.

Необхідним є існування процедур перевірки складних клієнтських трансакцій. Для складних багатосторонніх платіжних систем у разі виникнення грошових втрат внаслідок пошкодження або спотворення економічної платіжної інформації, відповідальність повинна бути розподілена між самим банком, його клієнтами і третіми особами або іншими учасниками платіжної системи.

5. Адміністрування і управління інформаційною банківською системою.

Причиною виникнення ризиків у цьому аспекті використання банківських інформаційних систем є технічні збої у обладнанні та програмному забезпеченні; вплив зовнішніх ризиків на банківські електронні системи і бази даних; недостатня потужність банківської комп'ютерної автоматизованої системи; моральний знос елементів системи. До цього переліку можна також додати складнощі та відмінності у адмініструванні різних технічних стандартів та протоколів даних; недостатній захист електронних комунікацій, що використовуються; недостатня системна безпека та контроль за нею.

Рівень І.

Визначається характер зв'язку між банківською внутрішньою операційною системою (системами) та системами, що відповідає за зовнішні електронні послуги та іншу банківську діяльність (наприклад, банківський веб-сервер). Якщо такий зв'язок існує, то необхідна консультація спеціаліста з інформаційних систем з приводу питань безпеки банківської інформації.

Необхідними також є процедури перевірки посилань веб-сайту банку до інших веб-сайтів, до яких належать як зовнішні (сайти інших банків, клієнтів, агентів платіжних систем тощо), так і внутрішні (наприклад, веб-сайти філій банку), для підтримки їх актуальності.

Встановлюється наявність процедур реєстрації спроб неавторизованого доступу до інтегрованої банківської автоматизованої системи:

- повинна бути впроваджена автоматизована система реєстрації зовнішніх звернень;
- повинні бути переглянуті всі відомі випадки таких спроб і засвідчено, що про них було повідомлено керівництво банку.

Також повинно бути створено план реакції на непередбачувані випадки і затверджена група спеціалістів для усунення негативних наслідків таких випадків. Якщо існує така група спеціалістів, то повинні бути документально затверджені їхні права і обов'язки.

Визначається наявність порядків і процедур використання банківської електронної пошти (внутрішньосистемної і зовнішньої) з таких спрямувань:

- обміну інформацію між групами користувачів, що складаються з працівників банку, клієнтів тощо;
- визначеного допустимого характеру інформації, яка передається, для усунення можливостей порушення її конфіденційності у разі випадкового неточного адресування інформації.

Рівень ІІ.

Визначається, чи керівництвом банку (або підрозділу електронних банківських операцій) встановлені необхідні рівні доступу до інформації і програмного забезпечення для різних працівників банку та інших можливих користувачів банківських електронних інформаційних систем. Ці рівні повинні чітко розподілятись і виконуватись.

Контролюється, як і який банківський працівник може запитувати інформацію по банківських рахунках, надавати необхідні доручення і дані для здійснення банківських операцій.

Необхідним є створення програм клієнтського сервісу, підтримки і навчання. Ці програми повинні включати:

- необхідний навчальний і ознайомчий матеріал для клієнтів. Він повинен відповідати вимогам збереження конфіденційності банківської інформації;
- інформування клієнтів повинно проводитись вчасно і регулярно.

Необхідним є своєчасне складання і вдосконалення інструкцій для клієнтів стосовно електронних банківських послуг. До них належать інструкції з управління клієнтськими рахунками, інших особистих реєстраційних даних. Вони повинні також містити інформацію з користування електронною поштою, файлами даних тощо, якщо вони містять банківську інформацію.

Рівень ІІІ.

Банк повинен надавати гарантії безпеки і якості функціонування для клієнта будь-якої застосовуваної банком платіжної системи або системи передачі даних. Ці

гарантії повинні бути затверджені юристом банку.

6. Участь сторонніх розробників (треті особи).

Оскільки банківська економічна інформація є чутливою до зовнішнього впливу, тому при розробці, експлуатації та обслуговуванні інформаційної системи банку повинні бути враховані наступні чинники, що можуть бути причиною виникнення ризиків та можливих втрат з боку банку. Недостатній рівень компетентності сторонніх розробників елементів системи (або всієї системи) може бути причиною можливих втрат в майбутньому. Також внутрішні правила контролю можуть не розповсюджуватись на третіх осіб. Зокрема, повинні бути враховані наступні можливості: слаба технічна підтримка з боку сторонніх розробників електронних банківських систем та ухилення від відповідальності; умови підтримки і адміністрування взаємодіючих систем, що перебувають поза впливом банку-власника; помилки при нагляді за відносинами між декількома банками-учасниками спільних платіжних систем.

За цим напрямком дослідження можуть здійснюватись наступні процедури перевірки:

Рівень І.

Встановлюється, чи банк має формальні контракти з кожним стороннім розробником банківської технології, що впроваджується. В контрактах повинні бути передбачені наступні пункти:

- права доступу, власності, зміни та управління клієнтською та іншою конфіденційною банківською інформацією;
- гарантії сервісного обслуговування в разі виникнення проблемної ситуації;
- участь сторонніх субпідрядників та обслуговуючого персоналу, який може бути задіяний у впровадженні банківської електронної інформаційної системи;
- регулярний і актуальний контроль і доповнення можливостей і складу впровадженої системи;
- вимоги безпеки з боку сторони, що розповсюджує банківські електронні послуги (Інтернет-провайдери, телефонні компанії тощо).

Треті особи повинні бути зобов'язані не розповсюджувати конфіденційну банківську інформацію та нести за це відповідальність.

Рівень ІІ.

Визначається наявність заходів захисту від порушення ліцензійних прав на програмні засоби, які належать банку, але були передані в користування третім особам (клієнтам).

Рівень ІІІ.

Процедури спостережень для цього рівня не передбачені.

Також важливим є те, щоб у планах впровадження електронних систем враховувався повний спектр їх застосувань. В програмах управління ризиками повинна бути створена сукупність внутрішніх стандартів на кожному етапі впровадження і функціонування будь-якої електронної банківської системи. Перелік цих стандартів і можливих ризиків, що виникають на кожному етапі впровадження і функціонування електронної банківської системи наведений у наступній таблиці (табл. 1).

Таблиця 1. Стандарти управління ризиками у електронних інформаційних банківських системах

Стандарти	Ризики
Спеціальна група контролю підтверджує відповідність визначеним стандартам кожної електронної інформаційної системи стратегічному плану діяльності банку і проводить аналіз ризиків відповідно до здійснюваної діяльності	Системи можуть використовуватись без чітко визначеного стратегічного управління або без спеціальної програми управління ризиками Структура та зміст електронних систем надання банківських послуг і їх можливості можуть не відповідати потребам клієнта Керівництвом може бути недостатньо оцінені технологічні втрати і тарифи, що впливають на фінансовий стан банку
Керівництво банку перевіряє існуючі порядки і процедури проведення операцій і вносить корективи відповідно до участі в електронних системах передачі економічних даних	Порядки і процедури можуть не відповідати вимогам банківської діяльності, проведенню операцій, вимогам безпеки Існуючі системи недостатньо забезпечують захист конфіденційної електронної банківської інформації
Керівництво проводить необхідне навчання і підвищення кваліфікації працівників, що задіяні у роботі електронних систем надання банківських послуг; повідомляє їх про потенційні ризики використання електронних систем передачі банківської інформації і платіжних систем	Недосконале навчання може вплинути на управління і процес ведення банківської діяльності
Внутрішні і зовнішні програми перевірки діяльності застосовують альтернативні системи передачі електронної банківської інформації	Потенційна незахищеність специфічних систем може бути недостатньо оцінена в масштабі банку і суміжних електронних систем
Кожна електронна система або електронна активність спеціально розроблена відповідно до правових основ і є законною	Юридична сила електронних контрактів, угод і підписів може бути невизначеною Банківські дії можуть бути трактовані як такі, що не відповідають юридичним стандартам
Керівництво встановлює необхідні стандарти і процедури для загальної програми управління і використання електронних систем	Банк може мати неадекватний захист електронних комунікацій, а також недосконале адміністрування електронних систем Електронні системи морально зношуються і повинні бути технологічно вдосконалені у відповідності до існуючих ринкових стандартів Об'єм електронних систем може не відповідати потребам банку і клієнтів
Існує розроблений адекватний план дій у непередбачуваних і стихійних випадках	Недостатньо кваліфіковане планування впровадження електронних систем може стати причиною виходу з ладу електронних систем і програмного забезпечення Банк може бути юридично відповідальним за втрати клієнтів внаслідок збоїв у функціонуванні банківських електронних систем
Інформація захищена і банківські внутрішні системи адекватно захищені від втручань зловмисників як ззовні, так і зсередини	Зловмисники можуть здобути право доступу до конфіденційної банківської або клієнтської інформації, спотворювати її зміст і механізми доступу до неї,

	розповсюджувати комп'ютерні віруси в банківській інформаційній системі, або спричиняти іншу шкоду Зовнішні спроби проникнення у банківську систему не можуть бути вчасно відстеженні і попереджені Незахищена пересилка даних може скомпрометувати чутливу інформацію Послаблення контролю через несанкціонований фізичний доступ до системного обладнання і програмного забезпечення
Встановлені необхідні стандарти для адміністрування зовнішніх відносин і витоку банківської інформації	Менеджмент може бути неефективним у відносинах з третіми особами-постачальниками послуг для виконання критичних функцій Досконало побудоване внутрішнє управління може не впливати на третіх осіб-постачальників Керівництво банку може не враховувати труднощів у моніторингу відносин між декількома фінансовими інституціями, постачальниками, агентами, організаторами, клієнтами і іншими учасниками платіжної системи Електронні послуги банку можуть бути недосконалими або неповними якщо розробники або треті особи-постачальники (та інші учасники) фінансово нестабільні

Висновок. Отже, моніторинг використання банківських електронних інформаційних систем, зокрема їх технічних складових, є надзвичайно важливим фактором у забезпеченні надійності і ефективності здійснення діяльності сучасної банківської установи. Дані моніторингу електронних систем, аналіз первинних даних за визначених нами напрямками є одним з основних джерел інформації для прийняття управлінських рішень і складання програм управління ризиками у банківській діяльності.

Запропонована нами програма контролю ризиків при використанні банківських електронних інформаційних систем може бути реалізована відповідними установами, що в свою чергу сприятиме підвищенню функціональних та фінансових показників якості їх діяльності. Результати наведеного дослідження при їх впровадженні у навчальний процес підвисили зацікавленість студентів економічного профілю (спеціальностей «Фінанси та кредит», «Облік і аудит») при вивченні дисциплін «Гроші та кредит», «Банківські операції», «Основи банківської справи», «Інформаційні системи і технології у фінансово-кредитних установах».

Література.

1. Закон України «Про платіжні системи та переказ коштів в Україні» [Електронний ресурс]. — К.: Верховна Рада України. — Режим доступу: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2346-14>.

2. Галіцин В.К. Системи моніторингу: Монографія. — К.: КНЕУ, 2000. — 231 с.

3. Ткаченко М.І. Визначення групи ризиків, які виникають при використанні електронних інформаційних систем у фінансово-кредитних установах // Вісник Хмельницького Національного університету, №5, т. 2. (159). — Хмельницький, 2010 р. — С. 219–222.

Стаття надійшла до редакції 12.10.2010 р.