18. Дегтяренко, И. В. Алгоритм поиска интервалов монофрактальности в неоднородных фрактальных процессах [Текст] / И. В. Дегтяренко, А. М. Гарматенко // Збірник наукових праць ДонІЗТ. – 2014 – №37. – С.59-67.
19. Український фондовий ринок: впевненість, стійкість та зростання [Електронний ресурс] / Звіт НКЦПФР // № 468 від 03 квітня 2012 р. – Режим доступу: \www/: URL: http://www.nssmc.gov.ua/user_files/content/58/1340015412.pdf

УДК 338.26: 004.738.5(075) **М.В. Макарова**

РОЗВИТОК СИСТЕМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ ТА ЕЛЕКТРОННОГО БІЗНЕСУ В УМОВАХ НЕВИЗНАЧЕНОСТІ ТА РИЗИКУ

У статті описано теоретико-методичні підходи до вирішення завдань розвитку систем електронної комерції (СЕК) та електронного бізнесу (СЕБ) в умовах невизначеності та ризику.

Ключові слова: *Системи електронної комерції, системи електронного бізнесу, ризики розвитку систем електронної комерції і електронного бізнесу, стратегічні ризики, репутаційні ризики, ризики інформаційної безпеки.*

В статье описаны теоретико-методические подходы к решению задач развития систем электронной коммерции (СЭК) и электронного бизнеса (СЭБ) в условиях неопределенности и риска.

Ключевые слова. *Системы электронной коммерции, системы электронного бизнеса, риски развития систем электронной коммерции и электронного бизнеса, стратегические риски, репутационные риски, риски информационной безопасности.*

The article describes the theoretical and methodical approaches to the challenges of E-commerce systems (SEC) and E-business systems (SEB) under conditions of uncertainty and risk.

Keywords. *E-commerce systems, E-business systems, the risks of development of E-commerce systems and E-business systems, strategic risks, reputation risks, information security risks.*

Актуальність розробки теоретико-методичних підходів до вирішення завдань розвитку систем електронної комерції (СЕК) та електронного бізнесу (СЕБ) в умовах невизначеності та ризику зумовлена, насамперед, змінами в основних виробничих ресурсах, що відбулися протягом останнього півсторіччя в провідних економіках світу та очікуються у решті квазіпостіндустріальних економік, в тому числі, в українській. Крім того, такі підходи вкрай необхідні для урахування домінуючої ролі інформації та знань як виробничого ресурсу розвиненої соціально-економічної системи для коригування національних стратегій економічного розвитку країн загалом і підтримки їх бізнесу, зокрема. Біфуркація глобального економічного розвитку, високий ступінь змінюваності інформаційних технологій і ризикованості ведення бізнесу потребують урахування фактору невизначеності при обґрунтуванні діяльності систем електронної комерції (СЕК) та електронного бізнесу (СЕБ).

Метою нашого дослідження є обгрунтування теоретико-методичних підходів щодо розвитку систем електронної комерції (СЕК) та електронного бізнесу (СЕБ) в умовах невизначеності та ризику.

Постановка задачі. Для досягнення зазначеної мети було поставлено і вирішено такі завдання:

- узагальнення тенденцій сучасного існування систем

електронної комерції та електронного бізнесу в Україні і у світі;

- аналіз природи невизначеності, конфліктності та породжуваного ними ризику під час розвитку систем електронної комерції і електронного бізнесу, що дозволило узагальнити фактори такої невизначеності і конфліктності;

- обґрунтування методичних розробок і практичних рекомендацій з оцінки природи ризиків розвитку вітчизняних систем електронної комерції та електронного бізнесу, що, зокрема, реалізувалися у пропозиції принципів базових механізмів контролю розвитку СЕК і СЕБ на підприємстві;

- узагальнення і ранжування ризиків розвитку вітчизняних і зарубіжних СЕК і СЕБ за ступенем небезпечності;

- аналіз доцільності застосування різних методів оцінки ризику розвитку систем електронної комерції і електронного бізнесу, що дозволило зупинитися на методах експертної оцінки як найбільш релевантних для якісної оцінки таких ризиків та їх ранжування;

- аналіз можливості застосування методу аналізу ієрархій при побудові ієрархії інформаційних загроз інформаційних систем, в тому числі, СЕК і СЕБ за ступенем небезпечності, що дозволяє чітко визначити їх вразливості та мінімізувати ймовірність реалізації цих загроз;

- пропозиція методичного підходу до типологізації систем електронної комерції та електронного бізнесу з урахуванням ризикованості їх запровадження і розвитку і формування такої типології.

Методи дослідження. У роботі було застосовано такі загальнонаукові і спеціальні методи: аналізу, синтезу,

системного підходу, узагальнення, групування і класифікації, експертних оцінок, аналізу ієрархій, типологізації, порівняльного аналізу, контент-аналізу.

Основний виклад матеріалу. Викладемо логіку і отримані результати дослідження більш детально.

На його першому етапі був проаналізований світовий і український досвід розвитку систем електронної комерції та електронного бізнесу у термін 2000-2016 рр., що характеризувався високим рівнем невизначеності ринкового середовища і ризиків фінансово-економічного і соціально-політичного характеру. Проведений аналіз дозволив узагальнити тенденції сучасного існування таких систем. Вони полягають у такому:

- в останнє десятиріччя відбулося остаточне нівелювання різниці між успішними Інтернет-проектами (Yahoo!, Amazon.com, E-Bay) і традиційними компаніями за основними ринковими показниками (прибутком, вартістю акцій тощо);
- транснаціональні корпорації частину свого бізнесу масово перенесли в Інтернет-простір;
- господарські Web-практики перетворилися на знакове явище. Розповсюдження Web-технологій сприяло й зміні методів управління в некомерційних організаціях і у державній владі, появі електронних урядів;
- в інформаційно розвинених країнах нині найшвидше відбувається розвиток моделей електронної комерційної взаємодії в міжфірмовій оптовій торгівлі за напрямом B2B – business-to-business;
- у напрямі C2B (consumers-to-business) зміцнили позиції відомі торговельні бренди, перехопивши ініціативу у суто віртуальних Інтернет-крамниць, відбувається розкрутка попиту методами управління рефлексією споживачів у соціальних мережах;

- активізувалися основні тенденції розвитку інформаційної економіки в Uanet: питома вага українських користувачів Мережі у загальній кількості населення складала на початок 2016 року майже дві третини (62%) дорослого населення України. Частка Інтернет-користувачів серед людей 18-39 років в Україні сягнула 91% [1]. Однак, Інтернет-крамниці в Україні, на відміну від зарубіжних, мають специфіку свого розвитку. В країнах «золотого міл'ярду» до переліку провідних онлайнових крамниць найчастіше входять Інтернет-представництва реально існуючих роздрібних мереж. В Україні, навпаки, найбільш поширені суто віртуальні проекти електронної комерції, наприклад, онлайновий супермаркет Rozetka.ua, що має понад 800 000 унікальних відвідувачів на день [2]. Перехід гігантів традиційної торгівлі на прямі онлайнові продажі ще не відбувся: так, відома мережа роздрібної торгівлі в Україні «Фокстрот» у світовій павутині не входить й до десятки найбільших магазинів. З іншого боку, казати про серйозних гравців на ринку української електронної комерції не доводиться: торговельних електронних точок з річним товарооборотом більше мільйонів доларів в Україні біля сотні. І все ж таки фінансові кризи 2008-2011 і 2014-2015 років призвели до масового залучення пересічних українців до закупівель в Інтернеті.

Далі нами було досліджено природу невизначеності, конфліктності та породжуваного ними ризику під час розвитку систем електронної комерції та електронного бізнесу. Це дозволило узагальнити фактори такої невизначеності і конфліктності, до яких відносяться:

- швидкозмінність інформаційних технологій створення і підтримки систем електронної комерції та електронного бізнесу;

- багатоваріантність заходів проведення маркетингової політики підприємств через Інтернет;
- високий ступінь конкуренції на частині електронних ринків (виробництва обчислювальної техніки і програмного забезпечення, інформаційних ресурсів, надання послуг Інтернету тощо);
- суб'єктивний фактор (персонал створення і підтримки СЕК і СЕБ, необхідність постійного підвищення його кваліфікації).

Нами було досліджено ризики, породжувані невизначеністю і конфліктності під час розвитку систем електронної комерції та електронного бізнесу. До них віднесено:

- Стратегічні ризики. Вибір ступеня інтеграції системи дистанційного обслуговування клієнтів з інформаційною системою підприємства повинен чітко співвідноситися з кадровими, технологічними і фінансовими ресурсами підприємства, а не базуватися на прагненні «бути попереду конкурентів». При невірному виборі формування і підтримка СЕК і СЕБ виявляються невиправдано дорогими. На цьому ж етапі повинні бути враховані довгострокові перспективи розвитку СЕК і СЕБ шляхом розробки стратегії, що охоплюють планування ресурсів, прогнозування цільового ринку, формування нового функціонального контенту систем тощо. Без стратегії розвитку і планування СЕК і СЕБ буде складно вчасно приділяти увагу аспектам інформаційної безпеки і, внаслідок цього, реагувати на загрози у відповідності з процесом управління ризиками.
- Операційні ризики. Здійснення транзакцій за допомогою СЕК і СЕБ потенційно загрожує підприємствам фінансовими втратами, у разі успіху шахрайських операцій або через системні збої. Причиною таких випадків

найчастіше виявляється все ж таки незадовільна інтеграція СЕК і СЕБ стороннього розробника у власну інформаційну систему підприємства. У такій ситуації увесь збиток припадає на підприємство, що запроваджує СЕК і СЕБ. Зазвичай операційні ризики функціонування СЕК і СЕБ вміщують:

- ризик персоналу – ризик витрат через помилки співробітників, шахрайство, недостатню кваліфікацію персоналу, несприятливі зміни у трудовому законодавстві тощо;
- ризик процесу – ризик витрат, пов'язаний із помилками в процесах проведення операцій і розрахунків за ними, їхнього обліку, звітності, ціноутворення тощо;
- ризик технологій – тут витрати зумовлені недосконалістю вживаних технологій. Для СЕК і СЕБ вони конкретизуються у: неякісній роботі провайдера; обриванні зв'язку під час проведення транзакції в електронний спосіб; відмовах в обслуговуванні тощо. Рішенням таких проблем є вибір якісного провайдера, використання відповідних засобів криптозахисту, розмежування прав доступу до інформації персоналу оператора торговельного майданчика. Більше того, деякі компанії забезпечують страхування таких ризиків;
- ризики середовища – ризики витрат, пов'язані з нефінансовими змінами в середовищі, в якому діють СЕК і СЕБ – змінами в законодавстві і у системі оподатковування, політичними змінами тощо;
- ризики фізичного втручання у діяльність систем – стихійних лих, пожеж, пограбувань, тероризму тощо.

- Ризики невідповідності. Наявність СЕК і СЕБ на підприємстві потребує додаткової відповідності вимогам чинного законодавства та державних регуляторів фінансових транзакцій і обробки персональних даних, зокрема, тих, що відповідають вимогам інформаційної безпеки. Невиконання хоча б деяких з цих вимог породжує фінансові та репутаційні ризики для підприємства, так само, як і санкції відповідних регуляторів.

- Репутаційні ризики. Практичний досвід свідчить, що клієнти вкрай болісно ставляться до неякісної роботи СЕК і СЕБ. Тимчасове обмеження переліку заявлених онлайн-послуг, доступу до них або низька стійкість СЕК і СЕБ можуть викликати у широкого кола клієнтів негативне ставлення до підприємства в цілому. При оцінці операційних ризиків доступності СЕК і СЕБ для користувачів слід брати до уваги і репутаційні ризики, що можуть виникнути.

- Ризики інформаційної безпеки. Наявність СЕК і СЕБ привертає увагу кіберзлочинців, в арсеналі яких для несанкціонованого доступу до інформаційних систем є широкий і постійно оновлюваний набір технологічного інструментарію. Ризики інформаційної безпеки, що є частиною операційних, повинні бути детально проаналізовані. Стосовно них підприємствами повинен бути застосований повний цикл процесу управління ризиками.

- Кредитні ризики. Можливість кредитування через Інтернет поки не така поширена в Україні, як використання кредитних банківських карт, але в майбутньому може стати важливим інструментом розвитку клієнтської бази банків. У цьому випадку активізуються загрози, пов'язані з ідентифікацією клієнта, перевіркою його кредитоспроможності, достовірністю одержуваних

відомостей, забезпеченням конфіденційності переданої інформації тощо.

- Ризики ліквідності. СЕК і СЕБ дозволяють значно розширити базу клієнтів підприємства. Разом з тим завдяки Інтернету клієнти здатні легко порівнювати різні пропозиції і, виявивши найбільш вигідну, масово «переходити» від одного підприємства до іншого. Така можливість загострює конкуренцію на ринку торговельних і банківських послуг та створює для кожного підприємства додаткову загрозу кризи ліквідності.

- Цінові ризики. Можливість проводити за допомогою СЕК і СЕБ операції з цінними паперами або валютою роблять доступною спекулятивну діяльність, в тому числі, із застосуванням спеціальних технічних засобів. У такому випадку підприємства фінансового сектору піддаються ціновим загрозам, пов'язаним з брокерською діяльністю.

Надалі нами було обґрунтовано методичні розробки і висунуто практичні рекомендації з оцінки природи ризиків розвитку вітчизняних систем електронної комерції та електронного бізнесу. Зокрема, запропоновано принципи базових механізмів контролю розвитку СЕК і СЕБ на підприємстві.

Вони ґрунтуються на таких положеннях:

1. Життєво важливою для підприємства є максимально детальна фіксація всіх дій клієнта в СЕК і СЕБ, операцій з його банківським рахунком, в першу чергу – транзакцій. Така фіксація, яка ведеться автоматично інформаційною системою підприємства, полегшує вибудовування послідовності подій при розслідуванні можливих інцидентів. Журнали подій у СЕК і СЕБ повинні зберігатися підприємством таким чином, щоб максимально забезпечити їх конфіденційність, цілісність і доступність.

Неможливість опротестувати реалізовану транзакцію забезпечується за допомогою сучасних засобів захисту інформації. Засоби інфраструктури «відкритих ключів» істотно знижують вірогідність того, що клієнт успішно спробує зняти з себе відповідальність за нібито не проведений ним платіж.

2. За таких умов контроль з боку служб інформаційної безпеки підприємства вимагає додаткової уваги до саме аспектів аутентифікації, фіксації дій в СЕК і СЕБ і неможливості їх опротестування, особливо для підприємств банківського сектору. Сучасна тенденція мінімізації процедур аутентифікації клієнта в СЕК і СЕБ підвищує ризик втрати репутації системи інформаційної безпеки підприємства в цілому.

3. Важливо при запланованій зміні технології аутентифікації в СЕК і СЕБ проводити відповідну оцінку можливого збитку. Впроваджувати зміни в цьому випадку слід тільки після відповідної оцінки можливих втрат і сприйняття ризику керівництвом підприємства.

4. Провідне місце в стратегії управління ризиками підприємства повинні зайняти принципи управління супутніми репутаційними ризиками, пов'язаними із забезпеченням конфіденційності персональних і банківських даних клієнтів. Підприємства повинні докладно інформувати клієнтів про свою політику у відношенні такої інформації: роз'яснювати цілі, для якої ці дані необхідні, повідомляти в загальних рисах про засоби їх захисту. Обробка клієнтської інформації має проводитися тільки в інформаційних системах високого ступеня захищеності.

5. Разом з тим підприємство має забезпечувати постійну доступність сервісів СЕК і СЕБ, як і здійснення підтримки користувачів в будь-який час.

Усі згадані ризики підлягають вимірюванню, незалежно від їх природи (кількісної чи якісної). Методи, що вимірюють ризик, можна класифікувати на загальні й спеціальні; кількісні і якісні. Загальні методи виміру ризику застосовуються незалежно від сфери діяльності підприємств. До них належать:

- статистичний метод;
- метод аналізу доцільності витрат;
- аналітичний метод;
- метод експертної оцінки;
- метод аналогів.

Спеціальні методи вимірюють ризик певної діяльності.

Якісні методи – це методи виміру з допомогою експертного аналізу. Кількісні методи характеризуються отриманням кількісної оцінки, що є зручною для інтерпретації економістами.

Вважаємо, що для кількісно вимірюваних ризиків розвитку систем електронної комерції і бізнесу придатні статистичний метод виміру, метод аналізу доцільності витрат, аналітичний. Для вимірювання якісних ризиків слід застосовувати методи експертної оцінки і метод аналогів.

Нагадаємо, через те, що при кількісній оцінці ризики враховуються у вигляді зменшення грошового потоку, але часто інформації для визначення розмірів можливих відхилень від бажаного результату і ймовірності їх виникнення недостатньо, при оцінці проектів створення систем електронної комерції і бізнесу виконується якісна оцінка ризику та їх ранжування.

Зазвичай це відбувається у відповідності до методу експертної оцінки, наприклад, за десятибальною шкалою від 1 (великий ризик) до 10 (малий ризик). Кожен член

експертної групи має дати свої оцінки ризиків, потім усереднені оцінки ризиків за кожним проектом створення або модернізації системи електронної комерції (бізнесу) зводяться, супроводжуються стислими коментарями і включаються до бізнес-плану.

Для виявлення найбільш небезпечних для розвитку СЕК і СЕБ ризиків нами було проведено обґрунтування їх ранжування за ступенем небезпечності (табл.1).

Таблиця 1.

Ранжування ризиків розвитку вітчизняних і зарубіжних СЕК і СЕБ за ступенем небезпечності

Ранг	Характеристика ризиків за небезпечністю
1	2
1.	Стратегічні ризики. Помилковість у виборі системи віддаленого обслуговування клієнтів призводить до низького ступеню її інтеграції з інформаційною системою підприємства, робить систему електронної комерції компанії невиправдано дорогою. Без стратегії розвитку і планування складно вчасно приділяти увагу аспектам інформаційної безпеки і внаслідок цього – реагувати на загрози у відповідності з процесом управління ризиками, що робить стратегічні ризики найбільш небезпечними серед усіх.
2.	Репутаційні ризики – можливість повної або часткової втрати ділової репутації підприємства внаслідок дії різних зовнішніх і внутрішніх факторів, що спричиняє зниження або повну втрату вартості репутаційних активів, а також фінансові втрати (у вигляді збитків або недоотриманого прибутку) та/або падіння ліквідності підприємства [3]. Як зазначено вище, клієнти болісно ставляться до неякісної роботи СЕК і СЕБ, що може виявлятися у тимчасовому обмеженні переліку заявлених онлайн-послуг, доступу до них або низькій стійкості СЕК і СЕБ. Це може викликати у клієнтів негативне ставлення до підприємства в цілому, а не тільки до його системи електронної комерції чи бізнесу. Репутаційні ризики враховуються й при оцінці операційних ризиків. Така подвійність репутаційних ризиків призводить до їх другого рангу у групі оцінюваних ризиків за небезпечністю.

Продовження табл. 1

1	2
3.	Операційні ризики виникають під час поточного функціонування СЕК і СЕБ, це ризики прямих або непрямих втрат, викликаних помилками або недосконалістю процесів у цих системах, помилками або недостатньою кваліфікацією персоналу підприємства або несприятливих зовнішніх подій нефінансової природи, наприклад, шахрайства або стихійного лиха). Множинність природи операційних ризиків з'ясовує їх високий третій ранг у рейтингу.
4.	Ризики інформаційної безпеки є частиною операційних ризиків. Саме для СЕК і СЕБ загрози з боку кіберзлочинців з їх арсеналом постійно оновлюваного набору технологічного інструментарію для несанкціонованого доступу є найчастішими, що ставить їх на четверте місце у рейтингу. Проявами таких ризиків є ризики зламування засобів криптозахисту; атаки на бази даних електронних торговельних систем; витік конфіденційної інформації тощо.
5.	Ризики невідповідності. Функціонування СЕК і СЕБ на підприємстві потребує відповідності вимогам чинного законодавства та державних регуляторів фінансових транзакцій і обробки персональних даних, зокрема, тих, що відповідають вимогам інформаційної безпеки. Невиконання вимог несе для підприємства фінансові та репутаційні ризики, так само як і санкції відповідних регуляторів. Тут можна згадати як різновид і ризик невідповідності якості продукції, що постачається.
6.	***Кредитні ризики – це невизначеність щодо повного та своєчасного виконання позичальником своїх зобов'язань згідно з умовами кредитної угоди. Кредитний ризик характеризує економічні відносини, що виникають між двома контрагентами — кредитором і позичальником – з приводу перерозподілу фінансових активів. Оскільки між кожною парою контрагентів складаються власні відносини, які не повторюються і не можуть бути виміряні точно, то процес оцінювання кредитного ризику досить складно піддається формалізації. Кредитний ризик має певні особливості, котрі повинен брати до уваги менеджмент підприємства під час управління [4].***

	Як знову ж таки зазначалося, Інтернет-кредитування поки не таке поширене в Україні, як використання кредитних банківських карт, але в майбутньому може стати важливим інструментом розвитку клієнтської бази банків. Тоді активізуються загрози, пов'язані з ідентифікацією клієнта, перевіркою його кредитоспроможності, достовірності одержуваних відомостей, забезпеченням конфіденційності переданої інформації та багато інших.
7.	Ризики ліквідності.
8.	Цінові ризики.

На підставі вищенаведеного нами запропоновано методичні рекомендації для підприємств, що запроваджують СЕК і СЕБ, з розробки стратегії проведення електронної комерції на підприємстві з точки зору оцінки стратегічних ризиків як найнебезпечнішої групи ризиків.

Нами розглянуто і проаналізовано метод аналізу ієрархій для оцінки ризиків інформаційної безпеки (РІБ) загалом і ризиків розвитку систем електронної комерції та бізнесу зокрема. Як загальновідомо, впровадження інформаційних технологій супроводжуються можливими порушення режимів інформаційної безпеки (ІБ). У найзагальнішому вигляді РІБ – це небезпека виникнення збитків, пов’язаних зі створенням, передачею, зберіганням та використанням інформації. На даний час в світі для оцінки РІБ використовується стандарт ISO/IEC 27005:2008. Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки [5]. Своє відображення стандарт знайшов у постанові Правління Національного банку України від 28.10.2010 № 474 «Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України» і у галузевому стандарті Національного банку України СОУ

Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» [6, 7].

Аналіз РІБ є інструментом, що дозволяє визначити:

• які об'єкти і в якій мірі потребують захисту;

• вартість засобів захисту, без використання яких система ІБ не може бути ефективною.

Загальноприйнятої методики якісної і кількісної оцінки РІБ не існує. Це пов'язано у першу чергу з відсутністю достатнього об'єму статистичних даних про ймовірності реалізації того чи іншого РІБ. Як зазначалося, в теперішній час найбільше розповсюдження отримала якісна оцінка РІБ, коли за відсутності точних даних значення параметрів встановлює експерт, що здійснює аналіз РІБ.

Методогічною проблемою є визначення найбільш небезпечних інформаційних загроз за допомогою розрахунку вагових коефіцієнтів при оцінці РІБ з використанням добре відомого в теорії прийняття рішень методу аналізу ієрархій (МАІ). Один з можливих підходів з використання МАІ при оцінці РІБ викладений у роботі [8].

Нагадаємо, метод аналізу ієрархій – математичний інструмент системного підходу до складних проблем прийняття рішень. МАІ не надає особі, що приймає рішення, будь-якого «вірного» рішення, а дозволяє йому в інтерактивному режимі знайти такий варіант, який найкращим чином узгоджується з його розумінням сутності проблеми та вимогами до її вирішення.

МАІ дозволяє зрозумілим і раціональним чином структурувати складну проблему прийняття рішень у вигляді ієрархії, порівняти і виконати кількісну оцінку альтернативних варіантів рішення.

Для дослідження РІБ можна побудувати ієрархічну структуру їх оцінки. Для її аналізу необхідно провести

розрахунки вагових коефіцієнтів інформаційних загроз з використанням МАІ. Будується дев'ятибальна шкала відносної важливості елементів ієрархії (інформаційних загроз та їх груп). За цією шкалою можна провести попарні порівняння кожної інформаційної загрози у власній групі та груп загроз відповідно таблиці 2.

Таблиця 2.

Шкала відносної важливості кожної інформаційної загрози [9]

Відносна важливість	Визначення
1	Однакова важливість
3	Помірна перевага одного над іншим
5	Сильна перевага
7	Значна перевага
9	Дуже сильна перевага
2,4,6,8	Проміжні рішення між двома сусідніми судженнями
Зворотні величини	Якщо при порівнянні А ті Б отримано одне з вищезазначених значень (х), то при порівнянні Б та А отримана зворотна величина, тобто (1/х).

Визначення ймовірності необхідно для підрахування рівня ймовірності успішної атаки, що залежить від потенціалу загрози, яка створюється активним джерелом загрози. Побудуємо для нашого прикладу для дев'яти інформаційних загроз трьох груп таблицю показників ваги ймовірності успішної атаки (табл. 3).

Таблиця 3.

Матриця порівняння інформаційних загроз для груп $I_1 – I_3$, складено автором за [8,9]

Група загроз I_1				Група загроз I_2				Група загроз I_3			
	Z_1	Z_2	Z_3		Z_4	Z_5	Z_6		Z_7	Z_8	Z_9
Z_1	1	1/2	1/3	Z_4	1	3	1/4	Z_7	1	5	3
Z_2	2	1	1/3	Z_5	1/3	1	1/6	Z_8	1/5	1	2
Z_3	3	3	1	Z_6	4	6	1	Z_9	1/3	1/2	1

Проведемо парні порівняння в кожній з таблиць. Парні порівняння – це оцінки (якісні або кількісні) відношення пріоритету одного вузла до пріоритету іншого, тобто результати парних порівнянь – це оцінки важливості (переваги, ймовірності тощо) кожного вузла ієрархії. Результат парного порівняння – оцінка відношень «ваг» порівнюваних об'єктів («ваги» об'єктів чисельно виражають їх перевагу, оптимальність, значимість тощо). Мета парних порівнянь – визначення пріоритетів вузлів ієрархії [9]. Вузол – це загальна назва для всіх альтернатив, головного критерію рейтингування рішень, усіх факторів, від яких так чи інакше залежить рейтинг. Наступний крок полягає в обчисленні вектору пріоритетів за матрицями кожної групи інформаційних загроз. У математичних термінах це – обчислення головного власного вектору, що після нормалізації стає вектором пріоритетів (табл. 4).

Таблиця 4 .

Шкала значень рівня ймовірності реалізації інформаційної загрози для СЕК і СЕБ, складено автором за [8,9]

Групи інформаційних загроз	Інформаційні загрози	Пріоритети відносно своєї групи	λ_{max}	Індекс узгодженості (ІУ)	Відношення узгодженості (ВУ)
1	2	3	4	5	6
I_1	Z_1	0,246	3,61	0,304	0,53
	Z_2	0,309			
	Z_3	0,445			
I_2	Z_4	0,219	3,07	0,036	0,06
	Z_5	0,093			
	Z_6	0,688			
I_3	Z_7	0,654	3,17	0,086	0,15
	Z_8	0,198			
	Z_9	0,148			

Розрахунок максимальних власних значень для кожної групи інформаційних загроз λ_{max} здійснюється відносно до матриці парних порівнянь: підсумовується кожен стовпець суджень; сума першого помножується на величину першої компоненти нормалізованого вектора пріоритетів; сума другого помножується на другу компоненту тощо; отримані числа складають.

Далі вводяться кількісні показники для визначення пріоритетів інформаційних загроз. Матриця порівнянь – таблиця числових значень парних порівнянь. Індекс узгодженості (ІУ) визначають як:

$$ІУ = (\lambda_{max} – n) / (n – 1), \quad (1)$$

де λ_{max} – максимальне власне значення;

n – число порівнюваних елементів (розмір матриці).

Індекс узгодженості – це кількісна оцінка суперечливості результатів порівнянь. Далі підраховується середнє значення ІУ для отриманої матриці (табл. 4).

Якщо розділити ІУ на значення випадкової узгодженості (ВУ-сть), то отримується відносна узгодженість (ВУ). Відносна узгодженість – відношення індексу узгодженості до середньостатистичного значення індексу узгодженості при випадковому виборі коефіцієнтів матриці порівнянь. Відносна узгодженість для системи в цілому характеризує зважене середнє значення відносної узгодженості з усіх матриць порівнянь. Для матриці n=3 ВУ-сть =0,58 [9]. Розраховується відношення:

$$ВУ=ІУ/ ВУ\text{-сть} \quad (2).$$

Значення відносної узгодженості, що менше або рівне 0,10, можна вважати придатним.

За допомогою даних, наведених в таблиці 5, можна порівняти групи інформаційних загроз для розвитку СЕК і СЕБ та визначити найбільш значущі з них.

Таблиця 5.

Попарне порівняння груп інформаційних загроз, складено автором за [8,9]

Групи інформаційних загроз	I_1	I_2	I_3
1	2	3	4
I_1	1	1/3	1/6
I_2	3	1	2
I_3	6	1/2	1

Наступний крок – записують групи загроз з пріоритетністю та відповідно визначають ступінь небезпечності групи (табл.6).

Для більш наочного надання даних можна побудувати діаграму визначення найбільш небезпечної групи інформаційних загроз (рис. 1).

Таблиця 6.

Пріоритетність груп інформаційних загроз СЕК і СЕБ, складено автором за [8,9]

Групи інформаційних загроз СЕК і СЕБ	Пріоритет	Ступінь небезпечності (ранг)
I_1	0,106	3
I_2	0,498	1
I_3	0,396	2

З використанням даних таблиці 6 та рисунку 1 визначається найбільш небезпечна група інформаційних загроз. Для цього прикладу це група I_2. Використовуючи дані таблиці 4, визначають найнебезпечніші інформаційні загрози. У прикладі це – Z_3, Z_6 та Z_7. Далі може бути побудована ієрархія інформаційних загроз СЕК і СЕБ за

ступенем небезпечності. Це дозволить менеджменту підприємств, що реалізують проекти електронної комерції і бізнесу, чітко визначити вразливості та мінімізувати ймовірність реалізації цих інформаційних загроз.

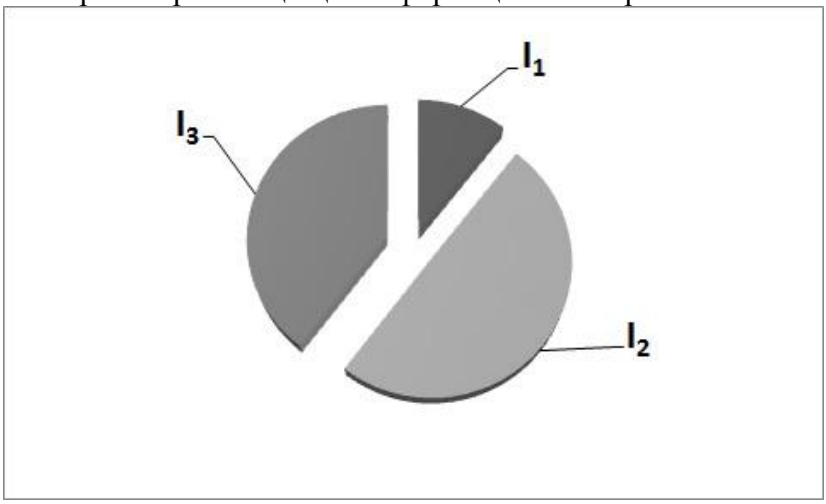

Рис. 1. Розподіл небезпечності груп інформаційних загроз розвитку СЕК і СЕБ, складено автором

На підставі вищевикладеного методичного підходу до оцінки ризиків інформаційної безпеки розвитку СЕК і СЕБ можлива побудова простого практичного інструментарію у програмному середовищі.

У межах дослідження також обгрунтувано методичний підхід до типологізації систем електронної комерції та електронного бізнесу з урахуванням ризикованості їх запровадження і розвитку, що реалізований за умови вирішення таких часткових завдань:

- обгрунтуваннння критеріїв типологізації СЕК і СЕБ за рівнем ризикованості розвитку;

- формування типології СЕК і СЕБ з урахуванням ризикованості їх розвитку.

Нагадаємо, що у бізнес-процесах систем електронної комерції та електронного бізнесу найчастіше задіяні такі різновиди учасників:

1. державні установи (Administration (далі – A, інколи G – Government)), а саме: міністерства, відомства, судові, державні представницькі, виконавчі та контролюючі органи тощо;
2. бізнес-структури (Business, далі – B): акціонерні товариства, приватні підприємства, промислово-фінансові групи, банки тощо;
3. споживачі (Consumer, далі – C): фізичні особи.

До складу систем електронного бізнесу, крім вищеперерахованих, можуть входити також такі суб'єкти як партнер (Partner), співробітник компанії (Employer).

При класифікації видів економічної діяльності, що здійснюється із використанням глобальної комп'ютерної мережі Інтернет, за суб'єктним складом учасників відносин найчастіше виділяють такі найбільш розвинені СЕК і СЕБ:

1. B2B (від англ. «Business-to-Business» або «бізнес-для-бізнесу») включає усі рівні взаємодії між компаніями з метою здійснення оптової купівлі-продажу товарів і послуг у режимі on-line;
2. B2C (від англ. «Business-to-Consumer» або «бізнес-для-споживача»), основою якої електронна роздрібна торгівля;
3. B2A (від англ. «Business-to-Administration» або «бізнес-для-адміністрації») – форма бізнесових транзакцій між компаніями та урядовими організаціями;
4. C2A (від англ. «Consumer-to-Administration» або «споживач-для-адміністрації») – сфера доступу громадян

до соціальної інформації та проведення простих трансакцій;

5. C2C (від англ. «Consumer-to-Consumer" тобто «споживач-для-споживача») – співтовариство споживачів, організоване з метою взаємної купівлі-продажу товарів і послуг.

Нині найбільш освоєними і масштабними є системи типу B2B та B2C.

Усі вищенаведені угрупування систем електронної комерції та електронного бізнесу не враховують ризикованості створення і функціонування СЕК і СЕБ і не включають її як ознаку розподілу на класифікаційні підгрупи.

У таблицях 7 і 8 нами проведено виокремлення критеріїв типологізації систем електронної комерції та електронного бізнесу та їх організаційно-економічних форм за ступенем ризикованості розвитку у розрізі різних ризиків [10, 11].

За нашою думкою, критерії типологізації сучасних систем електронної комерції та електронного бізнесу з урахуванням ризикованості можуть бути визначені матричним методом за рахунок співставлення проранжованих ризиків розвитку таких систем та їх вищенаведених класифікацій (табл. 9 і 10).

Таким чином, типологізація окремих СЕК і СЕБ та їх організаційно-економічних форм за ступенем ризикованості розвитку можлива на підставі, насамперед, формування критеріїв віднесення окремих груп їх класифікацій до тієї чи іншої групи за рівнем прояву цієї ознаки (таблиці 9 і 10).

Таблиця 7.

Виокремлення критеріїв типологізації систем електронної комерції та електронного бізнесу за ступенем ризикованості розвитку у розрізі різних ризиків

Номер рангу ризику	Тип ризику	Класифікації систем ЕК та ЕБ за певними ознаками												
		За сферою діяльності		За масштабами охоплення				За формою власності				За метою функціонування (за структурою бізнес-портфеля)		
		Оптова торгівля	Роздрібна торгівля	Локальні	Національні	Регіональні	Глобальні	Приватні	Державні	Змішаної форми власності	Основний спосіб ведення бізнесу	Диверсифікація існуючого бізнесу	Переорієнтація на нові види бізнесу, допоміжний бізнес	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	
1.	Стратегічний	+++**)	+++*)	+***)	+++	++	+++	+++	++	++	+++	++	+	+
2.	Репутаційний	++	+++	+	+++	++	+++	+++	+	++	+++	++	+	+
3.	Операційний	++	+	+	+++	++	+++	+++	+	++	+++	++	+	+
4.	Інформаційної безпеки	++	+++	+	+++	++	+++	+++	++	++	+++	++	+	+

Продовження табл. 7

1	2	3	4	5	6	7	8	9	10	11	12	13	14
5.	Невідповідності	++	+++	+	++ +	++	+++	+++	++	++	+++	++	+
6.	Кредитний	++	+++	+++	++	++ +	++	+++	+	++	+++	++	+
7.	Ліквідності	++	+++	+++	++	++ +	+	+++	+	++	+++	++	+
8.	Ціновий	+	+	+	+	++	++	+++	+	++	+++	++	+

*) +++ – високий рівень ризику
**) ++ – середній рівень ризику
***) + – низький рівень ризику

Таблиця 8.

Виокремлення критеріїв типологізації організаційно-економічних форм систем електронної комерції та електронного бізнесу за ступенем ризикованості розвитку у розрізі різних ризиків [11]

Номер рангу ризику	Організаційно-економічні форми систем електронної комерції та електронного бізнесу																	
	Тип ризику	Державний сектор економіки				Приватний сектор економіки												
		B2A	A2B	A2A	P2A	Великий бізнес				Середній бізнес				Малий бізнес				
						B2B	B2P	B2E	B2C	B2B	B2C	B2P	C2B	B2C	C2B	C2A	C2C	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
1.	Стратегічний	++	++	+	+	+++	+++	+	++	+++	+++	+++	++	+++	++	+	++	
2.	Репутаційний	+++	+	+	+	+++	+++	+	+++	+++	+++	+++	++	+++	++	+	+	
3.	Операційний	+	+	+	+	+++	+++	+	++	+++	++	+++	+	+++	+	+	++	
4.	Інформаційної безпеки	+++	+++	+++	++	+++	+++	+	++	+++	+++	+++	+	+++	+	+	+++	
5.	Невідповідності	+++	+++	+++	+++	+++	+++	+	++	+++	+++	+++	+	+++	+	+	++	
6.	Кредитний	+	+	+	+	+++	+++	+	++	+++	++	+++	+	++	+	+	+	
7.	Ліквідності	+	+	+	+	+++	+++	+	++	+++	++	+++	+	++	++	+	+	
8.	Ціновий	+	+	+	+	+++	+++	+	+	+++	++	+++	+	++	++	+	+	

Таблиця 9.

Типологізація систем електронної комерції та електронного бізнесу за ступенем ризикованості розвитку у розрізі різних ризиків [11]

Групи	СЕК і СЕБ	Різновид ризику							
		Стратегічний	Репутаційний	Операційний	Інформаційної безпеки	Невідповідності	Кредитний	Ліквідності	Ціновий
1	2	3	4	5	6	7	8	9	10
I. Найбільш ризикована група СЕК і СЕБ (7-8 ризиків з 8 має найвищий рівень)	Приватні	+++	+++	+++	+++	+++	+++	+++	+++
	Основний спосіб ведення бізнесу	+++	+++	+++	+++	+++	+++	+++	+++
II. Група СЕК і СЕБ з високим рівнем ризиків розвитку (4-6 ризиків з 8 має найвищий рівень)	Роздрібна торгівля	+++	+++	+	+++	+++	+++	+++	+
	Національні системи	+++	+++	+++	+++	+++	++	++	+
	Глобальні системи	+++	+++	+++	+++	+++	++	+	++
III. Група СЕК І СЕБ з середнім рівнем ризиків розвитку (2-3 ризиків з 8 має найвищий рівень)	Локальні системи	+	+	+	+	+	+++	+++	+
	Регіональні системи	++	++	++	++	++	+++	+++	++

Продовження табл.. 9

1	2	3	4	5	6	7	8	9	10
IV. Група СЕК і СЕБ з низьким рівнем ризиків розвитку (0-1 ризиків з 8 має найвищий рівень)	Оптова торгівля	++	++	++	++	++	++	++	+
	Державні системи	++	+	+	++	++	+	+	+
	Системи змішаної форми власності	++	++	++	++	++	++	++	++
	Диверсифікація існуючого бізнесу	++	++	++	++	++	++	++	++
	Переорієнтація на нові види бізнесу, допоміжний бізнес	+	+	+	+	+	+	+	+

Таблиця 10.

Типологізація організаційно-економічних форм систем електронної комерції та електронного бізнесу за ступенем ризикованості розвитку у розрізі різних ризиків [11]

Групи	СЕК і СЕБ	Різновид ризику								
		Стратегічний	Репутаційний	Операційний	Інформаційної безпеки	Невідповідності	Кредитний	Ліквідності	Ціновий	
1	2	3	4	5	6	7	8	9	10	
I. Найбільш ризикована група СЕК і СЕБ (7-8 ризиків з 8 має найвищий рівень)	Великий бізнес, напрями:									
	B2B	+++	+++	+++	+++	+++	+++	+++	+++	
	B2P	+++	+++	+++	+++	+++	+++	+++	+++	
	Середній бізнес, напрями:									
	B2B	+++	+++	+++	+++	+++	+++	+++	+++	
	B2P	+++	+++	+++	+++	+++	+++	+++	+++	
II. Група СЕК і СЕБ з високим рівнем ризиків розвитку (4-6 ризиків з 8 має найвищий рівень)	Середній бізнес, напрям B2C	+++	+++	++	+++	+++	++	++	++	
	Малий бізнес, напрям B2C	+++	+++	+++	+++	+++	++	++	++	

Продовження табл. 10

1	2	3	4	5	6	7	8	9	10
III. Група СЕК I СЕБ з середнім рівнем ризиків розвитку (2-3 ризиків з 8 має найвищий рівень)	Державний сектор економіки, напрями:								
	B2A	++	+++	+		+++	+++	+	+
	A2B	++	+	+		+++	+++	+	+
	A2A	+	+	+		+++	+++	+	+
IV. Група СЕК і СЕБ з низьким рівнем ризиків розвитку (0-1 ризиків з 8 має найвищий рівень)	Державний сектор економіки, напрям P2A	+	+	+		++	+++	+	+
	Великий бізнес, напрями:								
	B2E	++	++	++		++	++	++	++
	B2C	+	+	+		+	+	+	+
	Середній бізнес, напрями:								
	C2B	++	++	+		+	+	+	+
	Малий бізнес, напрями:								
	C2B	++	++	+		+	+	+	++
	C2A	+	+	+		+	+	+	+
	C2C	++	+	++		+++	++	+	+

Узагальнення результатів проведеної типологізації продемонструвало таке:

- сьогодні найбільш ризикованими групами СЕК і СЕБ, які потерпають від високого рівня практично усіх різновидів ризиків – від стратегічного до цінового, – є приватні системи зі сфери великого і середнього бізнесу організаційно-економічних форм B2B і B2P, для яких електронна комерція і електронний бізнес є основним способом ведення бізнесу;
- до групи СЕК і СЕБ з високим рівнем ризиків розвитку відносяться національні і глобальні системи, в першу чергу, роздрібної торгівлі зі сфери середнього і малого бізнесу організаційно-економічної форми B2C;
- група СЕК і СЕБ з середнім рівнем ризиків розвитку вміщує системи локального і регіонального масштабу дії усіх організаційно-економічних форм, а також СЕК і СЕБ, що належать до державного сектору економіки організаційно-економічних форм B2A, A2B, A2A, тобто ті, де відбувається взаємодія бізнесу і влади та адміністрацій між собою;
- найменш ризикованими СЕК і СЕБ нині є державні системи, системи змішаної форми власності і комерційні системи, за рахунок яких відбувається диверсифікація існуючого бізнесу компаній, переорієнтація на нові види бізнесу або ведеться допоміжний бізнес.

Якщо акцентувати на організаційно-економічних формах, то найменш ризикованими нині є СЕК і СЕБ у державному секторі економіки напряму P2A, у великому бізнесі – напрямів B2E і B2C (останній, мабуть, за рахунок вже досить тривалої історії розвитку і напрацювання своїх форм і методів), у середньому бізнесі – напряму C2B, у малому – напрямів C2B, C2A, C2C.

Цілком зрозуміло, що межі типологізації з плином часу змінюються, окремі різновиди ризиків стають менш критичними для тієї чи іншої системи електронної комерції чи бізнесу, однак, сьогодні запропонована типологізація стане в нагоді практичним менеджерам в якості інструменту для оцінки ризикованості прийняття рішення щодо запровадження певної СЕК або СЕБ.

Висновки.

Таким чином, наше дослідження з обгрунтування теоретико-методичних підходів щодо розвитку систем електронної комерції (СЕК) та електронного бізнесу (СЕБ) в умовах невизначеності та ризику дійшло певних результатів у вигляді вирішення поставлених завдань, а саме, нами було:

- узагальнено тенденції сучасного існування систем електронної комерції та електронного бізнесу в Україні і у світі, що продемонструвало високий рівень їх залежності від невизначеності ринкового середовища і ризиків фінансово-економічного і соціально-політичного характеру та певних національних особливостей запровадження Інтернет-технологій;
- проаналізовано природу невизначеності, конфліктності та породжуваного ними ризику під час розвитку систем електронної комерції і електронного бізнесу, що дозволило узагальнити фактори такої невизначеності і конфліктності, до основних з яких віднесено швидкозмінність інформаційних технологій створення і підтримки СЕК і СЕБ; багатоваріантність заходів проведення маркетингової політики підприємств через Інтернет; високий ступінь конкуренції на частині електронних ринків; суб'єктивний фактор;
- обґрунтувано підхід до оцінки природи ризиків розвитку вітчизняних систем електронної комерції та

електронного бізнесу, що, зокрема, реалізувалися у пропозиції принципів базових механізмів контролю розвитку СЕК і СЕБ на підприємстві. Так, незалежно від природи ризиків (якісної чи кількісної), базові механізми контролю розвитку СЕК і СЕБ на підприємстві мають ґрунтуватися на таких принципах: максимально детальній фіксації у журналі усіх дій клієнта в СЕК і СЕБ із забезпеченням їх конфіденційності, цілісності і доступності; додаткової уваги служб безпеки підприємств до аспектів аутентифікації, неможливості опротестування дій в СЕК і СЕБ; управління супутніми репутаційними ризиками, пов'язаними із забезпеченням конфіденційності персональних і банківських даних клієнтів; забезпечення постійної доступності сервісів СЕК і СЕБ та підтримки користувачів;

- проведено узагальнення і ранжування ризиків розвитку вітчизняних і зарубіжних СЕК і СЕБ за ступенем небезпечності. Так, тут виокремлено, насамперед, стратегічні, репутаційні, операційні ризики, ризики інформаційної безпеки, невідповідності, кредитні ризики, ризики ліквідності і цінові ризики. Найбільш небезпечними для розвитку СЕК і СЕБ підприємств загалом визначено стратегічні і репутаційні ризики, що, зокрема, дозволило запропонувати принципи розробки стратегії проведення електронної комерції на підприємстві з точки зору оцінки стратегічних ризиків як найнебезпечнішої групи ризиків;

- продемонстровано доцільність застосування різних методів оцінки ризику розвитку СЕК і СЕБ, незалежно від їх природи (кількісної чи якісної), а свідчать, що для кількісно вимірюваних ризиків придатні статистичний метод виміру, метод аналізу доцільності витрат, аналітичний. Для вимірювання якісних ризиків

(наприклад, репутаційних), ефективні методи експертної оцінки. Однак, через те, що при кількісній оцінці ризики враховуються у вигляді зменшення грошового потоку, а даних для визначення відхилень від запланованого результату діяльності СЕК і СЕБ недостатньо, при розгляді таких проектів виконується і якісна оцінка ризику, тобто методи експертної оцінки нині найбільш придатні для «вимірювання» і ранжування усіх ризиків розвитку СЕК і СЕБ;

- застосовано метод аналізу ієрархій при побудові ієрархії інформаційних загроз розвитку інформаційних систем, в тому числі, СЕК і СЕБ, за ступенем небезпечності, що дозволяє визначити найбільш небезпечні інформаційні загрози та їх групи і внаслідок цього мінімізувати ймовірність їх реалізації;
- обгрунтовано методичний підхід до типологізації систем електронної комерції та електронного бізнесу з урахуванням ризикованості їх запровадження і розвитку, що реалізований на підставі фасетної класифікації СЕК і СЕБ за різними ознаками, класифікування організаційно-економічних форм СЕК і СЕБ, обгрунтуваннння критеріїв типологізації СЕК і СЕБ за рівнем ризикованості розвитку, за ними сформовано типологію СЕК і СЕБ, що дозволило визначити групи найбільш ризикованих систем. Такий методичний підхід та його інструментарій стане в нагоді при практичній реалізації підприємствами своїй проектів електронної комерції та електронного бізнесу.

Основні результати нашого дослідження за темою знайшли відображення в публікаціях [11-16].

Список використаних джерел

1. Кількість інтернет-користувачів в Україні перевищила 60%: [Електронний ресурс]// Інформаційний сайт ZN,UA. – Електрон. дані. – Режим доступу: http://dt.ua/TECHNOLOGIES/kilkist-

internet-koristuvachiv-v-ukrayini-perevischila-60-207572_.html. – Назва з екрана. – Дата звернення: 16.06.16.

2. О нас [Електронний ресурс]// Офіційний сайт Інтернет-крамниці ROZETKA. – Електрон. дані. – Режим доступу: http://rozetka.com.ua/about/. – Назва з екрана. – Дата звернення: 17.06.16.
3. Важенина И.С. Риски деловой репутации: идентификация и оценка/ И.С. Важенина, С.А. Пестриков, Т.Р. Шарипов // Экономический анализ: теория и практика. – 2011. – №17 (224). – С. 2–11.
4. Примостка Л.О. Фінансовий менеджмент у банку: підручник / Л.О. Примостка. — 2-ге вид., доп. і перероб. — К.: КНЕУ, 2004. — 468 с.
5. ISO/IEC 27005:2008. Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки.
6. Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України: Постанова Національного банку України від 28.10.2010 N 474. [Електронний ресурс]. – Електрон. дані. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/v0474500-10. – Назва з екрана. – Дата звернення: 17.06.16.
7. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги: СОУ Н НБУ 65.1 СУІБ 1.0:2010. – [Чинний від 28.10.2010]. – К. : НБУ, 2019. – 59 с.
8. Замула О. А. Визначення найбільш небезпечних загроз в методиці оцінки інформаційних ризиків/ О.А. Замула, В.І. Черниш, Б.В. Волобуєв та інші// Інформаційно-керуючі системи на залізничному транспорті. – 2012. – №3. – С. 76-80.
9. Саати Т. Принятие решений. Метод анализа иерархий: пер. с англ. / Саати Т. – М.: «Радио и связь», 1993. – 278 с.
10. Креденець О.В. Засади формування системи електронної роздрібної торгівлі в Україні: автореф. дис. ... канд. екон. наук : 08.00.03 / О.В. Креденець; Центр. спілка спожив. т-в України, Львів. комерц. акад. – Львів, 2014. – 20 с.
11. Макарова М.В. Інформаційне забезпечення запровадження систем електронної комерції підприємств з урахуванням ризикованості їх розвитку/ М.В. Макарова// Зб. наук. праць «Економіко-математичне моделювання соціально-економічних систем». – К.: Міжнародний науково-навчальний центр

інформаційних систем і технологій НАН України та МОН України, 2015. – Випуск № 20. – С. 48-66.
12. Макарова М.В. Основні аспекти створення системи моніторингу діяльності господарюючого суб'єкта /М.В. Макарова// Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки. – Черкаси: ЧДТУ, 2012. – Вип. 31. – Ч. ІІ. – Т. 2. – С. 15-20.
13. Макарова М.В. Запровадження інформаційних систем управління персоналом в діяльність страхової компанії/М.В. Макарова, Т.І. Ручка // «Наукові праці Донецького національного технічного університету. Серія: економічна». – Донецьк.: ДНТУ, 2014.– № 4. – С.155-163.
14. Макарова М.В. Інформаційне забезпечення системи мониторінга діяльності господарюючого суб'єкта/М.В. Макарова// Збірник наукових праць ІІІ-а міжнародної науково-практичної конференції «Інформаційні технології і системи в документознавчій сфері». – Донецьк, ДонНУ, 2013 р. – С. 56-58.
15. Макарова М.В. Інформаційні системи у сучасній системі менеджменту промислових підприємств/ М.В. Макарова // Моделювання регіональної економіки. Збірник наукових праць. – Івано-Франківськ: Плай, 2012. – № 2. – С.402-407.
16. Макарова М.В. Метод аналізу ієрархій у плануванні та прийнятті управлінських рішень при запровадженні інновацій у нафтосервісних підприємствах/ М.В. Макарова, А.А. Щербань// Збірник наукових праць «Економіко-математичне моделювання соціально-економічних систем». – К.: Міжнародний науково-навчальний центр інформаційних систем і технологій НАН України та МОН України, 2013. – № 4. – С. 122-130.

УДК 338.47 **Л.І. Бажан**

ФОРМУВАННЯ ІМОВІРНІСНИХ ХАРАКТЕРИСТИК ЕКОНОМІЧНОЇ СТІЙКОСТІ ТРАНСПОРТНО-ЛОГІСТИЧНОЇ СИСТЕМИ

Описано математичну модель формування імовірнісних характеристик економічної стійкості транспортно-логістичної системи на основі аналізу