*Р.Л. УС,*
*к.е.н., старший викладач кафедри інформаційного менеджменту,*
*Київський національний економічний університет ім. Вадима Гетьмана*

# Інспекційні методи аудиту інформаційних технологій

*Стаття присвячена дослідженню й узагальненню сукупності інспекційних методів аудиту інформаційних технологій. Надано рекомендації щодо практичного використання запропонованих інспекційних методів при проведенні аудиту ІТ–середовища організації як цілісної складної системи.*

***Ключові слова:*** *ІТ–аудит, методичне забезпечення ІТ–аудиту, метод ІТ–аудиту, інспекційні методи ІТ–аудиту.*

*Р.Л. УС,*
*к.э.н., старший преподаватель кафедры информационного менеджмента,*
*Киевский национальный экономический университет им. Вадима Гетьмана*

# Инспекционные методы аудита информационных технологий

*Статья посвящена исследованию и обобщению совокупности инспекционных методов аудита информационных технологий. Предоставлены рекомендации по практическому использованию предложенных инспекционных методов при проведении аудита ИТ–среды организации как целостной сложной системы.*

***Ключевые слова:*** *ИТ–аудит, методическое обеспечение ИТ–аудита, метод ИТ–аудита, инспекционные методы ИТ–аудита.*

*R.L. US,*
*Ph.D., Senior Teacher of the Informational Management Department, Vadym Hetman Kyiv National Economic University*

# IT–audit inspection methods

*Article is dedicated to research and compile aggregate of the IT–audit inspection methods. Attached recommendations for the practical use of the proposed inspection methods for auditing the IT environment of the organization as an integrated complex system.*

***Keywords:*** *IT–audit, IT–audit methodical maintenance, IT–audit method, IT–audit inspection methods.*

***Постановка проблеми.*** Відповідно до узагальненого визначення сутності аудиту інформаційних технологій (ІТ–аудиту) [4] метою його проведення є незалежна експертиза ІТ–середовища організації, а також надання його замовнику об'єктивного висновку і професійних рекомендацій на основі зібраних аудиторських доказів. При цьому під аудиторськими доказами розуміють виявлені і задокументовані у процесі виконання аудиторських процедур факти щодо об'єкта ІТ–аудиту.

Для збору аудиторських доказів у процесі аудиту інформаційних технологій його виконавці (ІТ–аудитори) вдаються до використання різноманітних інспекційних методів [2], сутність яких полягає у використанні виконавцем аудиту спеціальних методичних прийомів і способів обстеження.

Результати використання інспекційних методів при проведенні конкретних процедур (заходів) ІТ–аудиту мають бути належним чином задокументованими. При цьому під аудиторською документацією розуміють записи у формі відповідних документів (також вживається термін «робочі документи») щодо виконаних аудиторських процедур і виявлених суттєвих доказів.

Зважаючи на сучасне широке різноманіття арсеналу інспекційних методів ІТ–аудиту, а також беручи до уваги зростання необхідності проведення аудиту ІТ–середовища організацій як цілісної складної системи [5], доцільно узагальнити сукупність таких методів і виокремити з їх числа ті, що є найбільш необхідними і достатніми для високоякісного та професійного виконання відповідних аудиторських процедур.

***Метою статті*** є дослідження й узагальнення сукупності інспекційних методів аудиту інформаційних технологій, а також надання рекомендацій щодо їх практичного використання, зокрема, при проведенні аудиту ІТ–середовища організації як цілісної складної системи.

***Виклад основного матеріалу.*** Аналізуючи наукові і практичні джерела з проблематики аудиту інформаційних технологій, зокрема застосування інспекційних методів у процесі його проведення [1–14 та ін.], а також відповідно до узагальненої класифікації методів ІТ–аудиту [2], пропонуємо для збору аудиторських доказів при проведенні аудиту ІТ–середовища організації як цілісної складної системи використовувати такі інспекційні методи, як анкетування, інтерв'ю, фізична перевірка, побудова структурних схем, комп'ютеризована підтримка проведення аудиту, аудиторські тести, аудиторська вибірка та залучення інших експертів. Розглянемо їх детальніше.

Анкетування (Questionnaires) – метод отримання аудиторських доказів у процесі ІТ–аудиту шляхом письмового опитування (із застосуванням анкетних листів) конкретних виконавців бізнес–функцій в організації (від операторів бізнес–процесів до вищого керівництва), які використовують ІТ у повсякденній роботі або взаємодіють з ІТ–середовищем у будь–який інший спосіб. При цьому фокус–група опитуваних може бути максимально широкою. За рівнем достовірності отриманих аудиторських доказів анкетування поступається іншим інспекційним методам ІТ–аудиту, однак є одним із найчастіше вживаних.

На практиці цей метод зазвичай застосовують для отримання «грубого» (загального, поверхневого) уявлення про ІТ–середовище організації, його функціональні елементи, «вузькі місця» тощо. Результати анкетування слугують підґрунтям для виокремлення елементів ІТ–середовища, які потребують детальної аудиторської перевірки.

Для проведення анкетування аудитор має передати заздалегідь розроблені анкети керівникам структурних підрозділів в організації. Останні мають організувати самоопитування їх підлеглих і потім передати заповнені анкети аудитору. Респонденти можуть заповнювати анкети безпосередньо на робочому місці у зручний для них час, однак у межах встановленого аудитором строку їх повернення.

 

Анкет може бути як кілька тематичних, так і одна комплексна. Питання мають бути чіткими і максимально зрозумілими для більшості опитуваних та стосуватися ІТ–середовища організації в цілому з метою надання можливості аудитору сформувати загальне уявлення про його підсистеми, елементи, процеси тощо. У тексті анкети має бути роз'яснена специфічна термінологія (якщо така присутня у запитаннях), а також надана чітка інструкція щодо правильного її заповнення.

Зазвичай запитання анкет ставляться у закритій формі з метою отримання конкретної відповіді, яка цікавить аудитора. Кількість запитань має бути обмеженою, зокрема, таким чином, щоб обсяг анкети не перевищував трьох сторінок, для отримання максимально обдуманих і достовірних відповідей.

В анкетах обов'язково мають бути окремі графи для ідентифікації анкетованого, його посади і підрозділу, у якому він працює. Також до заповненої анкети опитувані мають додавати шаблони документів, з якими працюють у повсякденній роботі.

Інтерв'ю (Interview) – метод отримання аудиторських доказів у процесі ІТ–аудиту шляхом усного опитування конкретних виконавців бізнес–функцій в організації (від операторів бізнес–процесів до вищого керівництва), які використовують ІТ у повсякденній роботі або взаємодіють з ІТ–середовищем у будь–який інший спосіб. На практиці цей метод вважається одним із найефективніших для отримання достовірних аудиторських доказів, однак потребує ретельної підготовки, а також високих комунікативних і професійних навичок аудитора тощо.

Перед застосуванням цього методу аудитор повинен, по–перше, переконатись, що інформація, яку він очікує отримати у результаті проведення інтерв'ю, не може бути отримана в інший, простіший або ефективніший спосіб. По–друге, необхідно чітко визначити цілі проведення інтерв'ю, а також яким чином їх досягнення реалізує загальну мету та цілі ІТ–аудиту. По–третє, необхідно визначити персонал організації, який зможе найкращим чином забезпечити надання необхідної інформації з максимальним рівнем достовірності. Для встановлення таких респондентів можуть бути застосовані організаційні діаграми. По–четверте, аудитор має організовувати інтерв'ю таким чином, щоб інформацію загального характеру запитували на початку та вкінці інтерв'ювання, а конкретну (специфічну) – в середині.

З метою мінімізації будь–яких сторонніх впливів на зміст відповідей інтерв'ювання кожного респондента зазвичай проводиться аудитором індивідуально в окремому приміщенні. Запитання мають охоплювати всі ключові функціональні підсистеми ІТ–середовища організації, зокрема в тих аспектах, які цікавлять замовника ІТ–аудиту найбільше, відповідно до поставлених цілей, завдань та обмежень аудиту тощо. Вони зазвичай ставляться у відкритій формі з метою отримання вичерпної персональної відповіді, а також особистої думки і побажань опитуваного. Кількість запитань та час проведення інтерв'ю мають бути обмеженими і достатніми для отримання лаконічних відповідей щодо усіх важливих аспектів.

До найбільш загальних запитань інтерв'ю при проведенні ІТ–аудиту можна віднести такі:

– ПІБ, посада, підрозділ, де працює опитуваний;

– які функціональні обов'язки виконує опитуваний і в якому бізнес–процесі (або бізнес–процесах);

– якої інформації (постійної/періодичної, нормативно–довідкової, оперативної тощо) потребує опитуваний для виконання своїх обов'язків;

– яку інформацію генерує опитуваний і для яких цілей;

– яку інформацію опитуваний передає іншим співробітникам і для яких цілей;

– які ІТ застосовує опитуваний для виконання своєї роботи;

– яким чином опитуваний взаємодіє із співробітниками ІТ–підрозділу;

– які засоби ІТ–безпеки застосовує опитуваний у роботі;

– яких політик, правил, інструкцій щодо використання ІТ, зокрема ІТ–безпеки, повинен дотримуватись опитуваний;

– чи задоволений опитуваний використанням ІТ у роботі, яку користь вони приносять та як підвищують продуктивність і якість його праці;

– які складнощі, інциденти і проблеми із використанням ІТ виникали в опитуваного, як вони усувалися, за який період часу та якою була участь ІТ–підрозділу в їх вирішенні;

– які побажання хоче висловити опитуваний щодо покращення ІТ–середовища тощо.

Усі інтерв'ю при проведенні ІТ–аудиту мають ретельно готуватись, запитання до кожного опитуваного детально продумуватись. Зокрема, опитування співробітників різних підрозділів мають враховувати специфіку тих бізнес–процесів, в яких вони беруть участь. При цьому найбільша увага має бути приділена інтерв'юванню працівників ІТ–підрозділу як одного із основних джерел отримання необхідних аудиторських доказів щодо ІТ–середовища об'єкта аудиту.

Найважливішими аспектами для виявлення аудиторських доказів за допомогою інтерв'ю є такі: внутрішні і зовнішні інформаційні потоки, які забезпечують функціонування організації, а також її взаємодію з іншими зовнішніми об'єктами; стратегія розвитку ІТ–середовища для досягнення цілей бізнесу (ІТ–стратегія); програмне забезпечення (інформаційні системи, сервісні додатки тощо), яке застосовується для задоволення потреб бізнесу; сховища електронної інформації (сховища даних, бази даних, файл–сервери, поштові сервери, мережеві диски спільного користування, системи управління каталогами даних та ін.); реальні функції структурних підрозділів організації, їх взаємозв'язки і взаємозалежності тощо.

Фізична перевірка (Physical inspection) – метод отримання аудиторських доказів у процесі ІТ–аудиту шляхом фізичного (візуального) спостереження наявності, місця розташування, стану і використання матеріальних активів ІТ–середовища організації. При проведенні ІТ–аудиту фізичні докази завжди є більш значимі, ніж будь–які інші, тому їх забезпечення у достатньому обсязі має бути одним із пріоритетів аудитора. До об'єктів застосування цього методу слід віднести:

– приміщення серверних кімнат, дата–центрів (data center), комутаційних кімнат (або шаф), систем резервного/автономного енергозабезпечення, сховищ паперової документації (архівів, картотек та ін.), офісів і складів служб ІТ–підрозділу тощо;

– обладнання та комплектуючі – комп'ютерне, мережеве і телекомунікаційне обладнання, засоби ризик–менеджменту ІТ щодо захисту фізичного доступу (кодові замки офісних приміщень, персональні ключі доступу, камери спостереження та ін.), засоби охорони безпеки праці (детектори диму, вологи, вогнегасники) тощо;

– організаційну документацію (на паперових носіях) – положення про бізнес– та ІТ–стратегію, моделі й опис бізнес– та ІТ–процесів, положення про організаційну структуру та функціональні обов'язки персоналу ІТ–підрозділу, проектна документація щодо розроблення і впровадження ІТ, внутрішні правила, інструкції щодо ІТ–середовища організації тощо;

– операційну документацію (на паперових носіях) щодо розроблення і придбання програмного забезпечення, інформаційних систем та інших ІТ, сервісного обслуговування комп'ютерного обладнання й інших впроваджених інформаційних технологій, а також внутрішнього сервіс–менеджменту ІТ–інфраструктури (Service Desk), наприклад, «тікети» (tickets) служби технічної підтримки ІТ–підрозділу (вхідні запити від клієнтів ІТ–сервісів) тощо;

– внутрішній моніторинг ІТ–середовища (на паперових носіях) – звітність про динаміку навантажень на ІТ–інфраструктуру, мережевий «трафік», інциденти ІТ–інфраструктури (збої та поломки обладнання, ПЗ, інформаційних систем, мереж тощо), інциденти ІТ–підрозділу (помилкові, зловмисні або шахрайські дії ІТ–персоналу тощо), інциденти ІТ–безпеки (несанкціонований доступ, вірусні і мережеві атаки) та ін.

Найважливішими аспектами фізичної перевірки в ІТ–аудиті є такі, як: інвентаризація обладнання та комплектуючих ІТ–середовища організації; виявлення заходів ризик–менеджменту ІТ щодо фізичного доступу; дотримання норм ергономічності і безпеки робочого середовища користувачів ІТ та ін.

Побудова структурних схем (Flowcharts) – метод отримання аудиторських доказів у процесі ІТ–аудиту шляхом побудови (графічного зображення) структурних схем (блок–схем або моделей) складових ІТ–середовища організації (підсистем, функціональних елементів, процесів тощо). Це дає змогу найбільш наочно (ілюстративно), зокрема для замовника аудиту, виявити/відстежити сильні і слабкі сторони об'єкта аудиту (ІТ–середовища).

На практиці такий метод зазвичай застосовують для відстеження вузьких місць контролю ризиків ІТ–середовища (ІТ–ризиків). Для цього аудитор, перш за все, має обрати методику побудови структурних схем, яка б дозволила найбільш наочно і зрозуміло зобразити специфіку елементів середовища інформаційних технологій, виявлених ІТ–ризиків, впроваджених заходів ризик–менеджменту ІТ (ІТ–контролів) тощо. Далі аудитор має визначитись із достатнім рівнем деталізації для відображення усіх важливих елементів системи ризик–менеджменту ІТ (системи ІТ–контролів), але так, щоб структурні схеми не були перенасичені зайвим змістом. Потім необхідно побудувати головну схему (primary flowchart) функціональних елементів ІТ–середовища, так, щоб кожен з них був легко відстежуваним і зрозумілим. На останньому кроці на основі головної схеми необхідно побудувати структурні схеми контролю ІТ–ризиків (control flowchart).

Комп'ютеризована підтримка проведення аудиту (Computer assisted audit techniques – CAATs) – метод отримання аудиторських доказів у процесі ІТ–аудиту шляхом застосування відповідних програмних засобів. Нині як такі засоби можуть бути використані: функціонал програмного забезпечення замовника аудиту (наприклад, аналітичні функції інформаційних систем, СУБД, серверів, Service Desk тощо); утиліти для вилучення та оброблення даних (програмні агенти, сервісні додатки, «скрипти» тощо); спеціалізоване програмне забезпечення підтримки процесу аудиту та ін.

Застосування засобів комп'ютеризованої підтримки при проведенні заходів ІТ–аудиту забезпечує його виконавцю такі переваги: по–перше, можливості автоматизованого пошуку, перевірки, оцінювання, аналізу та генерування звітів щодо суттєвої для аудиторського висновку інформації; по–друге, можливості автоматизованого виконання повторюваних (рутинних) аудиторських процедур щодо даних на електронних носіях, зменшуючи при цьому ймовірність припускання помилок аудитором; по–третє, економію трудових, часових й інших ресурсів на проведення аудиту; по–четверте, загальне підвищення якості і достовірності результатів ІТ–аудиту тощо.

Доцільність і зростаюча необхідність застосування такого методу для збору аудиторських доказів обумовлена поглибленням комп'ютеризації бізнес–процесів організацій і, відповідно, інформації щодо їх виконання. Однак рішення про застосування тих або інших CAATs при проведенні заходів ІТ–аудиту обов'язково має бути узгодженим із його замовником.

Аудиторські тести (Audit tests) – метод отримання аудиторських доказів у процесі ІТ–аудиту шляхом проведення перевірки функціональних елементів ІТ–середовища організації із застосуванням контрольних тестів. Зазвичай такі тести готуються у вигляді таблиці, в одній із колонок якої зазначаються запитання (або об'єкти/цілі) контрольної перевірки (control objectives), а в іншій залишається місце для занесення виявленої аудитором відповіді або відмітки про виконання. На практиці розрізняють два види аудиторських тестів [3, 10, 12]: на відповідність (compliance tests) і деталізовані (substantive tests).

Тести на відповідність – призначені для вибіркової (поверхневої) перевірки функціональних елементів ІТ–середовища організації на предмет підтвердження або спростування їх відповідності встановленим стандартам, еталонним практикам, правилам тощо. Застосування в цих тестах методу аудиторської вибірки, який буде розглянутий далі, дозволяє більш раціонально використовувати ресурси аудиту, виявляючи в ІТ–середовищі найбільш «проблемні» елементи, не вдаючись до детального дослідження і аналізу кожної із його складових. Такі тести зазвичай застосовуються для перевірки відповідності системи ризик–менеджменту ІТ в організації прописаним політикам, правилам тощо. Наведемо приклади контрольних запитань тестів ІТ–аудиту на відповідність:

– чи виконується періодична зміна паролів доступу до інформаційних систем;

– чи виконується періодична перевірка автоматичних реєстрів системних і програмних помилок, вірусних та мережевих атак;

– чи допускаються зміни програм і даних неавторизованими користувачами тощо.

Деталізовані тести – призначені для більш глибокої (детальної) перевірки функціональних елементів ІТ–середовища організації, зокрема, на основі результатів проведених тестів на відповідність, з метою виявлення суттєвих помилок, упущень, порушень встановлених політик, правил, вимог тощо. Тобто на практиці обсяг необхідних деталізованих тес–

тів IT–аудиту визначають за результатами тестувань на відповідність. Наприклад, за результатами тестування системи ризик–менеджменту IT на відповідність прописаним політикам і правилам може виявитися потреба в більш детальному дослідженні і аналізі її окремих елементів (процесів управління доступністю систем, резервного копіювання даних тощо).

Аудиторська вибірка (Audit sampling) – метод отримання аудиторських доказів у процесі IT–аудиту шляхом відбору деякої множини елементів із генеральної сукупності даних щодо тих або інших функціональних складових IT–середовища організації з метою перевірки певних характеристик, що притаманні усій сукупності. Практичне застосування цього методу при проведенні аудиторських процедур має ряд таких переваг: по–перше, зниження ризику проведення надмірної кількості аудиторських заходів; по–друге, швидке опрацювання великих обсягів інформації щодо об'єкта аудиту на основі відібраної множини репрезентативних елементів із генеральної сукупності даних; по–третє, реалізація одного із головних принципів аудиту – «отримати необхідний мінімум аудиторських доказів, достатніх для формування думки аудитора».

Найбільш поширеними при проведенні заходів IT–аудиту є такі види аудиторської вибірки: вибірка за властивими характеристиками/атрибутами (attribute sampling), вибірка за невластивими характеристиками (variable sampling) і статистична вибірка (statistical sampling).

Вибірка за властивими характеристиками – застосовується, як правило, в аудиторських тестах на відповідність для відбору із генеральної сукупності даних множини елементів, яким притаманна певна атрибутика (тобто які відповідають певним критеріям, вимогам тощо). Наприклад, такий вид аудиторської вибірки може бути застосований для відбору транзакцій певного IT–процесу, дані яких повинні бути захищеними алгоритмом шифрування з метою подальшої їх детальної перевірки, зокрема щодо надійності цього алгоритму тощо.

Вибірка за невластивими характеристиками – застосовується, як правило, в аудиторських деталізованих тестах для відбору із генеральної сукупності даних множини елементів, яким притаманні певні відхилення від встановлених критеріїв, правил, вимог тощо. Наприклад, такий вид аудиторської вибірки може бути застосований для відбору транзакцій певного IT–процесу, які були виконані з порушенням встановленої процедури авторизації їх виконавця з метою формування аудиторської думки про загальний рівень ризик–менеджменту цього процесу тощо.

Вибірка статистична – може застосовуватись у різноманітних аудиторських процедурах. Її суть полягає у випадковому відборі (random selection) множини елементів із генеральної сукупності даних, за яким кожен елемент має однакові шанси потрапити у вибірку.

Залучення інших експертів/консультантів (Using the work of other experts/consultants) – метод отримання аудиторських доказів у процесі IT–аудиту шляхом застосування праці або рекомендацій різноманітних експертів. При цьому вони можуть бути як зовнішніми відносно організації (замовника аудиту), так і внутрішніми.

На практиці цей метод зазвичай застосовують у випадку необхідності залучення спеціальних фахових або галузевих знань та практичних навичок для професійного оцінювання певних аспектів IT–аудиту, в яких компетентність аудитора є недостатньою для отримання висновків належного рівня якості і достовірності. Також залучення інших експертів може застосовуватись з метою делегування частини роботи IT–аудитора на аутсорсинг для прискорення її виконання тощо.

Основною перевагою застосування цього методу є можливість зосередити ресурси IT–аудиту на найважливіших його аспектах, відповідно до поставлених цілей, завдань й обмежень аудиту тощо, а також підвищити загальний рівень обґрунтованості і впевненості у його результатах.

Однак недоліком є необхідність укладання ряду додаткових угод із замовником аудиту щодо меж застосування роботи залучених експертів, їх відповідальності, прав доступу тощо. Крім цього, результати роботи залучених експертів, а також думка аудитора щодо рівня їх надійності обов'язково мають бути зазначені в аудиторському висновку окремим параграфом із відповідними коментарями.

Рішення про застосування такого методу має прийматись та узгоджуватись із замовником аудиту належним чином (у документальній формі) до початку виконання аудиторських процедур. Оскільки якщо аудитор усвідомить таку необхідність пізніше, він може витратити значний обсяг часу, відведеного для проведення аудиторських процедур, на узгодження всіх формальностей із замовником та експертами. Тому кожного разу перед початком проведення IT–аудиту його виконавець обов'язково має розглянути необхідність і можливість залучення праці або консультацій інших експертів, оцінити їх кваліфікацію, компетентність, досвід, ресурси, незалежність та якість роботи тощо.

**Висновки**

Аудиторські докази, зібрані із застосуванням розглянутих вище інспекційних методів IT–аудиту, є важливим підґрунтям для формування аудиторського висновку і рекомендацій. Однак у конкретному випадку аудиту вони є лише первинним матеріалом, який потребує додаткового професійного оброблення із застосуванням різноманітних аналітичних методів аудиту інформаційних технологій з метою отримання об'єктивної аналітичної інформації (свідоцтв аудиту) щодо IT–середовища організації.

**Список використаних джерел**

1. Васильев Р.Б. Управление развитием информационных систем: стратегический аудит состояния информационных систем / Р.Б. Васильев, Н.Г. Кальянов, Г.А. Левочкина [Електрон. ресурс]. – Режим доступу: http://www.intuit.ru/department/itmngt/mandevisys/3/1.html

2. Лазарєва С.Ф. Методологічне і методичне забезпечення аудиту інформаційних технологій / С.Ф. Лазарєва, Р.Л. Ус // Формування ринкових відносин в Україні: зб. наук. праць. – К.: НДЕІ, 2012. – Вип. 1 (128). – С. 117–125.

3. Міжнародні стандарти контролю якості, аудиту, огляду, іншого надання впевненості та супутніх послуг (том 1, том 2): Видання 2010 року // Пер. з англ. – К. ТОВ «ІАМЦ АУ «Статус», 2010.

4. Ус Р.Л. Аудит інформаційних технологій – новий вид аудиту організацій / Р.Л. Ус // Формування ринкових відносин в Україні: зб. наук. праць. – К.: НДЕІ, 2013. – Вип. 1 (140).

5. Ус Р.Л. Моделі холістичного аудиту інформаційних технологій / Р.Л. Ус // Формування ринкових відносин в Україні: зб. наук. праць. – К.: НДЕІ, 2011. – Вип. 5 (120). – С. 147–153.

6. COBIT 4.1 // IT Governance Institute, 2007. – 196 p.

7. Enterprise Value: Governance of IT Investments – The Val IT Framework 2.0 // IT Governance Institute, 2008. – 119 p.

8. Information technology – Security techniques – Information security risk management – BS ISO/IEC 27005:2008 // BSI, 2008. – 64 p.

9. ITIL v.3 – Lifecycle Publication Suite // OGC, 2007. – 1200 p.

10. Introduction to IT Audit Student Notes // INTOSAI, 2007. – 45 p.

11. IT Methods Student Notes // INTOSAI, 2007. – 97 p.

12. IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals // ISACA, 2010. – 330 p.

13. The Business Model for Information Security // ISACA, 2010 – 73 p.

14. The Risk IT Framework // ISACA, 2009. – 107 p.

*Л.Л. ЛИТВИНЕНКО,*
*к.е.н., доцент кафедри менеджменту зовнішньоекономічної діяльності підприємств, Національний авіаційний університет*

# Управління потенціалом інтеграції авіакомпанії в умовах міжнародного конкурентного середовища

*У статті автором досліджені основні актуальні проблеми управління потенціалом інтеграції авіакомпаній в умовах загострення конкуренції на міжнародних ринках, визначені перспективи реалізації стратегій інтеграції для забезпечення довгострокового розвитку вітчизняних авіакомпаній, досліджено передумови та послідовність приєднання національних авіакомпаній до глобальних авіаційних альянсів, проаналізовані особливості поєднання взаємних інтересів авіакомпаній – учасниць альянсів і ризики співпраці авіакомпанії в альянсі.*

***Ключові слова:*** *потенціал інтеграції, авіакомпанія, управління потенціалом, стратегічний альянс.*

*Л.Л. ЛИТВИНЕНКО,*
*к.э.н., доцент кафедры менеджмента внешнеэкономической деятельности предприятий, Национальный авиационный университет*

# Управление потенциалом интеграции авиакомпании в условиях международной конкурентной среды

*В статье автором исследованы основные актуальные проблемы управления потенциалом интеграции авиакомпаний в условиях обострения конкуренции на международных рынках, определены перспективы реализации стратегий интеграции для обеспечения долгосрочного развития отечественных авиакомпаний, исследованы предпосылки и последовательность присоединения национальных авиакомпаний к глобальным авиационным альянсам, проанализированы особенности взаимного сочетания интересов авиакомпаний – участниц альянсов и риски сотрудничества авиакомпании в альянсе.*

***Ключевые слова:*** *потенциал интеграции, авиакомпания, управление потенциалом, стратегический альянс.*

*L.L. LYTVYNENKO,*
*Ph.D. associate professor of the Management of Foreign Economic Activity of Enterprises Department, Institute of Economics and Management, National Aviation University*

# Airline integration potential management in terms of international competitive environment

*In the article the author has investigated the main current problems of integration potential management of airlines in terms of increased competition in international markets, identified the prospects of implementation integration strategies providing long–term development of domestic airlines, researched the background and stages accession of national airlines to global airline alliances, analyzed peculiarities in combination of mutual interests of airlines participating in alliances and risks of airline cooperation in alliance.*

***Keywords:*** *integration potential, airline, potential management, strategic alliance.*

***Постановка проблеми.*** За сучасних умов авіакомпанії використовують різні варіанти співпраці з іншими авіапідприємствами, основними серед яких є: поглиблення партнерських відносин у межах маркетингових, стратегічних та глобальних авіаційних альянсів, укладання код–шерінгових та інтерлайн–угод, розвиток взаємовигідної співпраці з аеропортами тощо. Формування авіаційних альянсів підвищує стійкість авіакомпанії в умовах ризику, а також надає авіакомпаніям–партнерам доступ до нових ресурсів та дозволяє оптимізувати використання власного потенціалу через його ефективне комбінування з ресурсами партнерів. Авіаперевізники, які не використовують переваги різних форм співпраці, можуть значно сильніше відчувати на собі негативні зміни на ринку та бути менш гнучкими порівняно з тими, які задіяні в кооперaційних та інтеграційних процесах. Стратегічна співпраця в рамках авіаційних альянсів дозволяє авіакомпаніям суттєво зменшити витрати, пов'язані з веденням конкурентної боротьби, та спрямувати зекономлені кошти на власний розвиток. З огляду на це актуальною проблемою є ефективне управління потенціалом інтеграції авіакомпаній.

***Аналіз досліджень та публікацій з проблеми.*** Проблеми управління потенціалом підприємств широко досліджували зарубіжні та вітчизняні науковці, зокрема Н. Азанова, Р. Брун, Г. Гейл, Р. Делбрідж, З. Замір, Ф. Зафар, Т. Лін, М. Маркус, А. Піліпенко, А. Сахар, П. Седдон, К. Таніс, К. Хінкельман, А. Чапліна, Ш. Шанг [3, 6, 7]. Різноаспектний аналіз переваг та ризиків реалізації стратегій інтеграційного зростання шляхом приєднання до стратегічних та глобаль–

 