

Таблиця 2. Часові аспекти розробки і реалізації маркетингової стратегії нового туру

| Етапи розробки і впровадження маркетингової стратегії | Термін виконання |
|---|------------------|
| Визначення маркетингових цілей та стратегічних намірів їх досягнення | |
| Аудит відповідності стратегічних намірів умовам середовища бізнесу | |
| Розробка маркетингової стратегії | |
| Затвердження маркетингової стратегії | |
| Доведення інформації про завдання стратегії основним зацікавленим сторонам | |
| Здійснення вимірювань виконання маркетингової стратегії | |
| Аналіз, оцінка та перегляд підходів до розробки та реалізації маркетингової стратегії | |

Розробку маркетингової стратегії варто починати всередині календарного року, оскільки в кінці року її вже необхідно реалізовувати, це пояснюється насамперед сезонністю діяльності туристичної сфери та необхідністю розроблювати маркетингову стратегію щорічно, оскільки на потреби споживачів впливає велика кількість різних факторів.

Висновки

У статті розкрито особливості формування маркетингової стратегії для просування нового туристичного продукту туристичними агентами. Визначено основні етапи побудови маркетингової стратегії та часові аспекти її реалізації. Вище запропоновані заходи є практично обґрунтованими, і застосування даних заходів сприятиме зро-

станню фінансових вигод туристичних агентів у найближчому майбутньому.

Література

1. Котлер Ф. Маркетинг менеджмент: анализ, планирование, внедрение, контроль / Пер. с англ. О.А. Третьяк, Л.А. Волкова, Ю.Н. Каптуревский. – СПб.: Питер, 1999. – 896 с.
2. Куденко Н.В. Маркетингові стратегії фірми / Куденко Н.В. – К.: КНЕУ, 2002. – С. 13.
3. Ламбен Ж.Ж. Стратегический маркетинг. Европейская перспектива. Пер с франц. – СПб.: Наука, 1986. – 589 с.
4. Маркетинг туризму: навч. Посіб. – Ч. 2. – К.: Вид-во Європ. ун-ту. – 2006. – 427 с.
5. Правик Ю.М. Маркетинг туризму: підручник / Ю.М. Правик. – К.: Знання, 2008. – 303 с.

С.Ф. ЛАЗАРЄВА,
к.е.н., професор,
РЛ. УС,

асистент кафедри інформаційного менеджменту, Київський національний економічний університет ім. В. Гетьмана

Методологічне і методичне забезпечення аудиту інформаційних технологій

Стаття присвячена дослідженню й узагальненню світового і вітчизняного досвіду з методологічного і методичного забезпечення аудиту інформаційних технологій (ІТ-аудиту). Запропоновано модель системи методологічного забезпечення та узагальнену класифікацію методів ІТ-аудиту. Надано пропозиції щодо їх застосування в Україні.

Ключові слова: ІТ-аудит, методологічне забезпечення ІТ-аудиту, методичне забезпечення ІТ-аудиту, метод ІТ-аудиту, інспекційні методи ІТ-аудиту, аналітичні методи ІТ-аудиту.

Статья посвящена исследованию и обобщению зарубежного и отечественного опыта по методологическому и методическому обеспечению аудита информационных технологий (ИТ-аудиту). Предложена модель системы методологического обеспечения и обобщенная классификация методов ИТ-аудита. Приведены предложения их использования в Украине.

Ключевые слова: ИТ-аудит, методологическое обеспечение ИТ-аудита, методическое обеспечение ИТ-аудита, метод ИТ-аудита, инспекционные методы ИТ-аудита, аналитические методы ИТ-аудита.

Article is dedicated to investigation of the foreign and native experience of the methodological and methodical maintenance for the information technology audit (IT-audit). Proposed the model of the system of the methodological maintenance and generalized classification of the IT-audit methods. Attached the propositions about use of this maintenance in Ukraine.

Keywords: IT-audit, IT-audit methodological maintenance, IT-audit methodical maintenance, IT-audit method, IT-audit inspection methods, IT-audit analytical methods.

Постановка проблеми. Результативність діяльності організацій дедалі більше залежить від застосовуваних інформаційних технологій (ІТ). Це зумовлює зростання потреби у

підвищенні ефективності й економічності їх функціонування, збільшення переваг і зменшення недоліків від використання, а також обґрунтування відповідних інвестицій в ІТ тощо. Тому дедалі більшого значення і поширення набуває такий інструмент інформаційного менеджменту, як аудит інформаційних технологій (ІТ–аудит). Теоретичними і прикладними розробками у сфері ІТ–аудиту займаються нині ряд організацій, у тому числі міжнародних. У країнах Заходу, зокрема у США, навчання і сертифікація фахівців з аудиту інформаційних технологій здійснюється відповідними професійними інститутами за спеціально розробленими програмами. Однак в Україні ця сфера аудиторської діяльності перебуває на стадії емпіричного накопичення знань і методів.

Метою статті є дослідження й узагальнення світового і вітчизняного досвіду та надання пропозицій щодо застосування методологічного і методичного забезпечення аудиту інформаційних технологій в Україні.

Виклад основного матеріалу. Під методологічним забезпеченням аудиту інформаційних технологій будемо розуміти сукупність правил, принципів й інших норм щодо організації та порядку здійснення цього виду аудиторської діяльності на належному професійному рівні. Його джерелами є стандарти, кодекси професійної етики, керівництва тощо [1–20]. Методологічне забезпечення ІТ–аудиту має загальний характер, його принципи є обов'язковими до виконання суб'єктами та об'єктами аудиту, яких воно стосується.

У світовому масштабі розробниками такого забезпечення є міжнародні й державні організації та громадські професійні об'єднання. Вони ж здійснюють сертифікацію фахівців і контроль рівня знань та практичного застосування відповідних нормативних документів. Відповідно методологічне забезпечення ІТ–аудиту має три рівні: міжнародний, національний і професійний.

Методологічне забезпечення ІТ–аудиту міжнародного рівня має на меті уніфікувати таку діяльність та гармонізувати умови міждержавної взаємодії у цій сфері. До його складу пропонуємо відносити стандарти, кодекси професійної етики, програми навчання тощо, розроблені міжнародними інституціями (табл. 1).

Аналіз методологічного забезпечення ІТ–аудиту міжнародного рівня показує, що найвагоміший внесок в його створення і розповсюдження, а також у розвиток концепції ІТ–аудиту в цілому зробила міжнародна організація ISACA. Нині лише вона працює безпосередньо над розробкою й удосконаленням методологічного забезпечення саме аудиту інформаційних технологій, зокрема стандартів та кодексів професійної етики ІТ–аудитора тощо. Також асоціація одна з небагатьох проводить глобальну сертифікацію фахівців з ІТ–аудиту за рядом кваліфікацій: сертифікований аудитор інформаційних систем (Certified Information System Auditor – CISA); сертифікований менеджер з інформаційної безпеки (Certified Information Security Manager – CISM); сертифікований фахівець із стратегічного управління інформаційними

технологіями організації (Certified in the Governance of Enterprise IT – CGEIT); сертифікований фахівець з контролю ризиків та інформаційних систем (Certified in Risk and Information Systems Control – CRISC).

Інші організації або пропонують стандарти, які лише опосередковано стосуються аудиту інформаційних технологій, або ж обмежуються проведенням тренінгів і розробкою керівництв загального навчального характеру у цій сфері.

Наступний рівень методологічного забезпечення аудиту інформаційних технологій – національний. Пропонуємо до нього відносити стандарти, кодекси професійної етики, практичні керівництва, форми звітності, інструкції, положення й інше методологічне забезпечення ІТ–аудиту, розроблене і затверджене уповноваженими державою інститутами.

Залежно від особливостей законодавства кожної країни, національне методологічне забезпечення ІТ–аудиту можуть розробляти як вищі органи нагляду за професією аудитора (аудиторською діяльністю), так і професійні аудиторські об'єднання, державні організації із стандартизації, науково–дослідні інститути у сфері інформаційних технологій, інформаційної безпеки та ін. Як правило, таке забезпечення розробляється у відповідності з міжнародним, для досягнення максимальної сумісності з ним. Вищі органи нагляду за професією аудитора у тій або іншій країні за дорученням уряду зазвичай виконують такі функції [1, 2, 5, 8–11]: затвердження національних нормативів аудиту (стандартів, кодексів етики тощо); навчання й атестація осіб, які бажають займатися аудиторською діяльністю; сертифікація аудиторів; ведення реєстру аудиторів та їх організацій; розгляд суперечок та застосування дисциплінарних заходів; контроль за дотриманням аудиторами вимог законодавства, стандартів аудиту, норм професійної етики тощо; контроль незалежності зовнішніх аудиторів та якості надання аудиторських послуг; співпраця з іншими аудиторськими організаціями (професійними, державними, міжнародними) та ін.

Аналіз показав, що глибина розробки методологічного забезпечення у різних країнах різна. Найбільші досягнення в його розвитку мають такі країни, як США, Великобританія, Німеччина, Австралія та ін. (табл. 2). Зокрема, найактивніше таке забезпечення розробляється і застосовується у США. Інші ж держави розробляють і впроваджують його, здебільшого, у якості рекомендацій ефективного управління ІТ (керівництв, специфікацій, моделей, методологій тощо), опосередковано обґрунтованих урядовими кодексами найкращих практик у сферах фондового ринку, банківської справи та ін.

Важливий принцип, яким варто керуватися, – розробка методологічних документів (методологічного забезпечення) національного рівня є необхідною лише за відсутності аналогічних документів на міжнародному рівні, або недостатнього висвітлення у міжнародних документах певних аспектів, важливих для тієї або іншої країни. У більшості ж випадків доцільніше керуватися міжнародними методологічними документами, вводити їх в дію на рівні державних або галузевих

ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗЕЙ ТА ВИДІВ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ

Таблиця 1. Міжнародне методологічне забезпечення аудиту інформаційних технологій

| Організація–розробник | Методологічний документ |
|--|---|
| <p>Міжнародна федерація бухгалтерів – МФБ (International Federation of Accountants – IFAC), створена у 1977 році. До її складу нині входять 164 діючі члени у 125 країнах світу. Вона об'єднує більше ніж 2,5 млн. фахівців у сфері аудиту і бухгалтерського обліку громадського сектору. В Україні єдиним дійсним членом цієї організації є Федерація професійних бухгалтерів і аудиторів України</p> | <p>Міжнародні стандарти аудиту – MCA (International Standards of Auditing – ISAs): 401 «Аудит середовища комп'ютерних інформаційних систем (Auditing in a Computer Information Systems Environment)»; 1008 «Оцінювання ризиків і внутрішнього контролю – EDP–характеристики і міркування, додаток №1 до MCA 400 (Risk Assessments and Internal Control – EDP Characteristics and Considerations, Addendum 1 to the ISA 400)»; 1009 «Засоби комп'ютеризованої підтримки аудиту (Computer-assisted Audit Techniques – CAATs)» та ін. Положення МФБ (IFAC Statements): 1001 «ІТ–середовище – автономні мікрокомп'ютери (EDP Environments – Stand-alone Microcomputers)»; 1002 «ІТ–середовище – он-лайн комп'ютеризовані системи (EDP Environments – On-line Computer Systems)»; 1003 «ІТ–середовище – системи баз даних (EDP Environments – Database Systems)» та ін. Керівні принципи ІТ–комітету МФБ (IT Committee of the IFAC Guidelines): «Управління інформаційною безпекою (Managing Security of Information)»; «Управління ІТ–планування ведення справ (Managing IT – Planning for transact)»; «Придбання інформаційних технологій (Acquisition of Information Technology)»; «Впровадження ІТ–рішень (The Implementation of IT solutions)»; «Надання і підтримка ІТ–послуг (IT service delivery and support)»; «ІТ–моніторинг (IT Monitoring)» та ін.</p> |
| <p>Міжнародна організація вищих органів фінансового контролю (The International Organization of Supreme Audit Institutions – INTOSAI), заснована у 1953 році. До її складу нині входять 189 повноцінних членів (вищих органів контролю державних фінансів) і чотири асоційованих. В Україні дійсним членом цієї організації є Рахункова палата (РП) України</p> | <p>Керівництва (Guides) і навчальні тренінги (Trainings, Student Notes), комітету INTOSAI з ІТ–аудиту (IT audit committee): «Основи ІТ–аудиту (Introduction to IT Audit)»; «ІТ–контролі (IT Controls)»; «ІТ–методи (IT methods)»; «ІТ–безпека (IT security)»; «Організація ІТ–аудиту та управління ним (Organization & Management of IT audit)»; «Планування неперервності бізнесу (Business continuity planning)»; «Засоби комп'ютеризованої підтримки аудиту (Computer Assisted Audit Techniques)»; «Завантаження і перетворення даних (Data downloading and conversion)»; «Аудит розробки систем (Auditing systems development)»; «Аудит ефективності ІТ–витрат (Value for money audit of IT)»; «Методологія перевірки безпеки інформаційної системи (Information system security review methodology)»; «Оцінка і аналіз ІТ–витрат (Cost estimation & analysis)» та ін.</p> |
| <p>«Асоціація аудиту і контролю інформаційних систем» (Information Systems Audit and Control Association – ISACA), заснована у 1969 р. Нині вона об'єднує більше ніж 95000 фахівців у більше ніж 160 країнах світу. Її членами є внутрішні і зовнішні аудиторів, виконавчі директори (CEOs), фінансові директори (CFOs), ІТ–директори (CIOs), педагоги, професіонали з ІТ–безпеки і контролю, ІТ–консультанти та ін. Найближча до України робоча група ISACA знаходиться в Росії</p> | <p>Стандарти ІТ–аудиту і надання впевненості (IT Audit and Assurance Standards): S1 «Договір про аудит» (Audit Charter); S2 «Незалежність (Independence)»; S3 «Професійна етика і стандарти (Professional Ethics and Standards)»; S4 «Компетентність (Competence)»; S5 «Планування (Planning)»; S6 «Виконання аудиторської роботи (Performance of Audit Work)»; S7 «Звітвання (Reporting)»; S8 «Супровід (Follow-Up Activities)»; S9 «Неналежні та незаконні дії (Irregularities and Illegal Acts)»; S10 «Стратегічне управління ІТ (IT Governance)»; S11 «Застосування оцінки ризику у плануванні аудиту (Use of Risk Assessment in Audit Planning)»; S12 «Суттєвість аудиту (Audit Materiality)» та ін. Кодекс професійної етики ІТ–аудитора (Code of Professional Ethics) – висуває до аудиторів вимоги щодо дотримання ключових етичних норм при виконанні професійних обов'язків, а також попереджає про відповідальність і дисциплінарні заходи. Стандарти професійного контролю інформаційних систем (IS Control Professionals Standards) – схожі за змістом до стандартів ІТ–аудиту. Керівні принципи ІТ–аудиту і надання впевненості (IT Audit and Assurance Guidelines): «Належна професійна турбота (Due Professional Care)»; «Документування аудиту (Audit Documentation)» та ін. Керівництва (Guides, Frameworks): «Процедури та техніки ІТ–аудиту і надання впевненості (IT Audit and Assurance Tools and Techniques)» та ін.</p> |
| <p>Інститут внутрішніх аудиторів (The Institute of Internal Auditors – IIA), заснований у 1941 році. Об'єднує нині близько 170 тис. фахівців у більше ніж 165 країнах світу. Членами цієї організації є фахівці з внутрішнього аудиту, ризик–менеджменту, внутрішнього контролю, ІТ–аудиту, освіти, безпеки та ін.</p> | <p>Практичні керівництва (Practice Guides, Global Technology Audit Guide – GTAG): «Управління інформаційною безпекою (Information Security Governance)»; «Аудит користувацького ПЗ (Auditing User-developed Applications)»; «Виявлення і запобігання шахрайству в автоматизованому середовищі (Fraud Prevention and Detection in an Automated World)»; «Аудит ІТ–проектів (Auditing IT Projects)» та ін. Звіт про придатність систем для проведення аудиту і контролю (Systems Auditability and Control (SAC) Report) – керівництво з поглибленого контролю та аудиту інформаційних систем і технологій. Підкреслює відповідальність менеджменту за визначення, і усвідомлення походження ризиків, пов'язаних з впровадженням інформаційних технологій в організації, а також за нагляд і контроль використання ІТ. Складається з 14 модулів: Середовище аудиту і контролю (Audit and Control Environment); Управління комп'ютерними ресурсами (Managing Computer Resources); Телекомунікації (Telecommunications); Безпека (Security) та ін.</p> |
| <p>Міжнародна організація із стандартизації (International Organization for Standardization – ISO), заснована у 1947 році. Об'єднує нині національні інститути із стандартизації 162 країн, з Центральним Секретаріатом у Женеві (Швейцарія). За час своєї діяльності організацією було опубліковано більше ніж 18 500 міжнародних стандартів</p> | <p>Міжнародні стандарти: ISO–900x «Система стандартів управління якістю (Quality management systems)»; ISO 15408 «Загальні критерії оцінювання ІТ–безпеки (The Common Criteria for Information Technology Security Evaluation)»; ISO 15504 «Визначення потенціалу ПЗ і процес його удосконалення (Software Process Improvement and Capability Determination – SPICE)»; ISO 17021:2006 «Оцінка відповідності. Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту (Conformity assessment. Requirements for bodies providing audit and certification of management systems)»; ISO 19011:2002 «Керівні принципи аудиту якості управління системами навколишнього середовища (Guidelines for quality and/or environmental management systems auditing)»; ISO–2000x «Система стандартів управління ІТ–послугами (Information technology – Service management)»; ISO 2700x «Система стандартів управління інформаційною безпекою (Information technology – Security techniques)»; ISO 31000 «Загальні керівні принципи впровадження ризик–менеджменту (General guidelines for principles and implementation of risk management)»; ISO 38500:2008 «Стандарт стратегічного управління ІТ (The IT Governance Standard)» та ін.</p> |

ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗЕЙ ТА ВИДІВ ЕКОНОМІЧНОЇ ДІЯЛЬНОСТІ

Таблиця 2. Національне методологічне забезпечення аудиту інформаційних технологій

| Країна | Методологічний документ |
|--|---|
| Організація-розробник | |
| США (USA) | |
| Американський інститут дипломованих громадських бухгалтерів (American Institute of Certified Public Accountants – AICPA) | Положення щодо стандартів аудиту (Statements on Auditing Standards – SASs) – забезпечують керівництва застосування загальноприйнятих стандартів аудиту AICPA (Generally Accepted Auditing Standards – GAAS), зокрема на виконання вимог Закону SOX: SAS Nos. 70 «Обслуговування організацій (Service Organizations)»; 94 «Вплив ІТ на аудиторську оцінку внутрішнього контролю при проведенні фінансового аудиту (The Effect of Information Technology on the Auditor’s Consideration of Internal Control in a Financial Statement Audit)»; 99 «Оцінювання випадків шахрайства при проведенні фінансового аудиту (Consideration of Fraud in a Financial Statement Audit)»; 107 «Ризик і суттєвість в аудиті (Audit Risk and Materiality in Conducting an Audit)»; 109 «Розуміння організації та її середовища, а також оцінювання ризиків і суттєвих помилок (Understanding the Entity and its Environment and Assessing the Risks of Material Misstatements)»; 115 «Порівняння внутрішнього контролю з критеріями аудиту (Communicating Internal Control Related Matters Identified in an Audit)» та ін. Специфікація «SysTrust», розроблена спільно з Канадським інститутом привілейованих бухгалтерів (Canadian Institute of Chartered Accountants – CICA) – є керівництвом оцінки надійності систем із застосуванням стандартизованих принципів і критеріїв |
| Наглядова рада за веденням фінансової звітності публічних компаній (Public Company Accounting Oversight Board – PCAOB) | Стандарти аудиту (Auditing Standards – ASs), на виконання вимог Закону SOX: AS Nos. 1 – перезатвердив усі загальноприйняті стандарти аудиту (GAAS), розроблені і впроваджені AICPA; 2 і 5 – затвердили модель COSO як основу оцінки ефективності системи і процедур внутрішнього контролю та ін. |
| Комітет спонсорських організацій комісії Тредвея (The Committee of Sponsoring Organizations of the Treadway Commission – COSO) | Модель внутрішнього контролю (Model of Internal Control), розроблена за сприяння і безпосередньої участі спонсорів COSO – професійних аудиторських організацій: Американської асоціації бухгалтерів (American Accounting Association – AAA), Інституту управлінського обліку (Institute of Management Accountants – IMA), Інституту внутрішніх аудиторів (IIA), Міжнародної асоціації фінансових директорів (The Financial Executives International – FEI) та AICPA – для оцінки ефективності системи і процедур внутрішнього контролю організацій. Керівництво з ризик-менеджменту організацій (Enterprise Risk Management) – розроблене, для застосування зовнішніми аудиторами, зокрема на виконання вимог Закону SOX, щодо запобігання шахрайству, для оцінки ефективності управління ризиками і системою внутрішнього контролю організацій |
| Національний інститут стандартів і технологій (National Institute of Standards and Technology – NIST) | Федеральні стандарти обробки інформації (Federal Information Processing Standards – FIPs), зокрема на виконання вимог Законів FISMA, E-Government та ін.: FIPS Nos. 186-3 «Стандарт цифрового підпису (Digital Signature Standard – DSS)»; 191 «Керівні принципи аналізу безпеки локальної мережі (Guideline for The Analysis of Local Area Network Security)»; 197 «Передовий стандарт з шифрування (Advanced Encryption Standard – AES)»; 200 «Мінімальні вимоги щодо безпеки федеральної інформації та інформаційних систем (Minimum Security Requirements for Federal Information and Information Systems)» та ін. Спеціальні публікації-керівництва (Special Publication 800 series): SP 800-12 «Основи комп’ютерної безпеки (An Introduction to Computer Security)»; SP 800-18 «Керівництво розробки планів безпеки для федеральних інформаційних систем (Guide for Developing Security Plans for Federal Information Systems)»; SP 800-53 «Рекомендовані контролю безпеки для федеральних інформаційних систем (Recommended Security Controls for Federal Information Systems)»; SP 800-53A «Керівництво оцінювання контролів федеральних інформаційних систем (Guide for Assessing the Security Controls in Federal Information Systems)» та ін. |
| Великобританія (United Kingdom) | |
| Британський інститут стандартів (British Standards Institution – BSI) | Стандарти: BS 5760 «Надійність систем, обладнання і компонентів (Reliability of systems, equipment and components)»; BS 7799 «Системи управління інформаційною безпекою – Специфікація з практичним керівництвом (Information Security Management Systems – Specification with guidance for use)»; BS 8900:2006 «Керівництво для управління стійкого розвитку (Guidance for managing sustainable development)»; BS 25999 «Управління неперервністю бізнесу (Business continuity management)»; BS 31100:2008 «Кодекс практики ризик-менеджменту (Code of practice for risk management)» та ін. Специфікація PAS-56 (Publicly Available Specification 56) – універсальне керівництво для управління неперервністю бізнесу. Визначає: процес, принципи і термінологію управління неперервністю бізнесу; забезпечує загальне середовище передбачення інцидентів і реагування на них; описує методики і критерії оцінювання та аналізу неперервності бізнесу |
| Управління TickIT Британського інституту стандартів (TickIT Office within BSI) | Програми сертифікації (Schemes): Tick IT та TickIT Plus – для акредитації систем управління якістю розробників програмного забезпечення, за підтримки UKAS та SWEDAC, а також для навчання і сертифікації TickIT-аудиторів під керівництвом IRCA. Керівництво TickIT Guide та ін. |
| Управління урядовою комерцією (Office of Government Commerce – OGC) | Методології та керівництва (Best Management Practice, Methods), розроблені, здебільшого, урядовою організацією Великобританії «Центральною комп’ютерно-телекомунікаційною агенцією (Central Computer and Telecommunications Agency – CCTA)», яка з 2001 року входить до складу OGC; більшість із них нині є зареєстрованими торговими марками, і розповсюджуються на комерційних засадах: «Бібліотека інфраструктури інформаційних технологій (Information Technology Infrastructure Library – ITIL®)» – нині один із стандартів de-facto у світовій практиці ІТ-менеджменту; «Проектування у контрольованому середовищі (PProjects IN Controlled Environments – PRINCE®, PRINCE2®) – процесно-орієнтована методологія проектного менеджменту, зокрема у сфері ІТ, із застосуванням структурного підходу; »Оцінювання ризиків та управління ними (CCTA Risks Assessment and Managing Method – CRAMM) – методологія визначення й аналізу інформаційних ризиків організацій та управління ними; «Структурний аналіз і проектування систем (Structured Systems Analysis and Design Method – SSADM®)» – методологія проектування інформаційних систем із застосуванням системного підходу; а також моделі і методології: M_o_R®, MSP®, P3O®, P3M3®, MoP™, MoP™, e-PIMS™ й інші |

| Німеччина (Germany) | |
|--|--|
| Федеральне управління інформаційною безпекою (Federal Office for Information Security – FOIS, нім. аббревіатура – BSI) | Стандарти (BSI–Standards): 100–1 «Система управління інформаційною безпекою (Information Security Management Systems – ISMS)»; 100–2 «Методологія ІТ–безпеки (IT–Grundschutz Methodology)»; 100–4 «Управління неперервністю бізнесу (Business Continuity Management)» та ін. Керівництва (Manuals, Guidelines): «Основа захисту ІТ: стандартні заходи безпеки (IT Baseline Protection Manual: Standard Security Measures)»; «Аудит інформаційної безпеки (Information security audit – IS audit)» та ін. |
| Австралія (Australia): | |
| Організація із стандартизації Австралії (Standards Australia) | Стандарти: AS/NZS 4360:2004 «Стандарт з ризик–менеджменту (Risk Management Standard)»; AS 8015–2005 «Стандарт корпоративного стратегічного управління інформаційно–комунікаційними технологіями (Standard for corporate governance of information and communication technology)» та ін. Керівництва: НВ 221:2004 «Управління неперервністю бізнесу (Business Continuity Management Handbook)»; НВ 436:2004 «Керівні принципи ризик–менеджменту (Risk management Guidelines)» та ін. |
| Австралійська дослідницька фундація бухгалтерів (Australian Accounting Research Foundation) | Стандарти аудиту: AUS 214 «Аудит у середовищі комп’ютерних та інформаційних систем (Auditing in a CIS Environment)» та ін. |

документів. Для цього зазвичай необхідно: по–перше, отримати офіційну згоду від розробника методологічного забезпечення (організації, яка його створила і розповсюджує), та, по–друге, здійснити його переклад на державну мову й адаптувати до вимог національного законодавства [5, 7].

Україна, взявши зазначений принцип на озброєння, затвердила і застосовує як національне методологічне забезпечення аудиторської діяльності, в тому числі й у сфері ІТ–аудиту, стандарти аудиту та етики Міжнародної федерації бухгалтерів (табл. 1). Згідно із Законом України «Про аудиторську діяльність» ці стандарти є обов’язковими для дотримання вітчизняними аудиторами, аудиторськими фірмами та суб’єктами господарювання.

Наступний рівень методологічного забезпечення аудиту інформаційних технологій – професійний. Пропонуємо до нього відносити стандарти, практичні керівництва (методології, моделі, керівні принципи тощо) та інше методологічне забезпечення ІТ–аудиту, розроблене професійними аудиторськими та іншими організаціями. Його зобов’язані застосовувати лише сертифіковані члени професійних організацій, решта ж фахівців – вільні керуватися ним на власний розсуд.

Професійне методологічне забезпечення ІТ–аудиту розвивається найбільш динамічно порівняно із національним та міжнародним; постійно вдосконалюється і доповнюється разом із розвитком самих інформаційних технологій. До розробки методологічного забезпечення ІТ–аудиту професійного рівня долучаються як спеціалізовані професійні організації у сфері аудиторської діяльності, так і організації, що займаються стандартизацією діяльності у сфері ІТ–менеджменту, а також великі корпорації ІТ–індустрії (табл. 3).

Професійні аудиторські організації діють у багатьох країнах світу. Вони об’єднують аудиторів у різноманітних сферах професійної спеціалізації. У сфері ІТ–аудиту нині найбільш відомою і значимою з таких організацій є Інститут стратегічного управління інформаційними технологіями (ITGI) у США, до складу якого з 2003 року входить професійна аудиторська організація Фундація аудиту і контролю інформаційних систем (ISACF).

ITGI з 1998 року займається розробкою практичних керівництв, в яких пропонує концептуальні основи, методоло-

гії, моделі, керівні принципи тощо ефективного стратегічного управління інформаційними технологіями організації (IT Governance). Вони засновані на найкращому досвіді з проектування, розробки, впровадження, управління й аудиту ІТ–організації; стандартах і найкращих практиках управління неперервністю бізнесу, системою якості, стійкого розвитку тощо; а також на загальновідомих методологіях ІТ–менеджменту, зокрема таких, як ITIL, PRINCE2, CMMI, PMBOK, TOGAF, та інших [12, 13, 19, 20].

Багато керівництв, розроблених інститутом, нині є стандартами de–facto у світовій практиці ІТ–менеджменту. Вони тісно взаємопов’язані одне з одним, а також зі стандартами ІТ–аудиту міжнародної організації ISACA. Цим формується єдиний методологічний комплекс для стратегічного управління інформаційними технологіями (IT Governance).

Нині у практичному середовищі ІТ–аудиту найбільш відомим керівництвом, розробленим ITGI, є «Контрольні об’єкти/цілі для інформаційних і пов’язаних з ними технологій» (Control Objectives for Information and related Technology – COBIT®). В його останній робочій версії – 4.1. пропонується не лише детально описана методологія організації і контролю (управління) ІТ–середовища, а й методологія проведення його аудиту.

Інститут позиціонує COBIT як бізнес–орієнтовану методологію високого рівня, метою якої є приведення ІТ–середовища організації у відповідність з її бізнес–цілями. Вона сконцентрована у більшій мірі на тому, що має бути досягнуто, ніж на тому, як досягнути ефективного управління і контролю ІТ.

Методологія пропонує базову референтну модель ІТ–процесів (IT Processes), які керують ІТ–ресурсами (IT Resources) організації для інформаційного забезпечення бізнесу, у відповідності з бізнес–вимогами (Business Requirements). Референтна модель ІТ–процесів COBIT 4.1 є ієрархією чотирьох (4) доменів (груп процесів – domains), які включають тридцять чотири (34) процеси (високорівневі об’єкти/цілі контролю – processes) та двісті десять (210) робіт (деталізовані об’єкти/цілі контролю – activities). Це дозволяє охопити весь спектр видів діяльності у сфері інформаційних технологій організації і забезпечити цілісне бачення її ІТ–середовища.

Таблиця 3. Професійне методологічне забезпечення аудиту інформаційних технологій

| Тип видавця | Методологічний документ |
|---|---|
| Організація-розробник | |
| Професійні організації у сфері аудиту і стандартів з ІТ-менеджменту | |
| Фундація аудиту і контролю інформаційних систем (Information Systems Audit and Control Foundation – ISACF), яка входить до складу IT Governance Institute – ITGI | Керівництва (Management Guidelines, Frameworks): «Концептуальна основа ІТ-аудиту і надання впевненості» (IT Assurance/Audit Framework – ITAF™); «Контрольні об'єкти/цілі для інформаційних і пов'язаних з ними технологій (Control Objectives for Information and related Technology – COBIT®)»; «Управління ефективністю ІТ-інвестицій організації (Enterprise Value: Governance of IT Investments – Val IT™)»; «Концептуальна основа управління ІТ-ризиками (The Risk IT Framework – Risk IT)»; «Бізнес-модель інформаційної безпеки (The Business Model for Information Security – BMIS™)» та ін. |
| Асоціація присяжних дипломованих бухгалтерів (The Association of Chartered Certified Accountants – ACCA) | Практичні керівництва (Papers of ACCA Study System) проведення аудиту у середовищі інформаційних систем і технологій організацій, засновані на міжнародних стандартах МФБ (IFAC): Paper Nos. 2.1 «Інформаційні системи (Information systems)»; 2.6 «Аудит і внутрішня перевірка (Audit and Internal review)»; 3.4 «Управління бізнес-інформацією (Business Information Management)» та ін. |
| Інститут системних адміністраторів, аудиторів, спеціалістів у комп'ютерних мережах та інформаційній безпеці (SysAdmin, Audit, Network, Security Institute – SANS) | Тренінгові курси (Training courses): AUD 429 «Основні елементи аудиту ІТ-безпеки (IT Security Audit Essentials)»; SEC 440 «20 критичних контролів безпеки: планування, впровадження та аудит (20 Critical Security Controls: Planning, Implementing and Auditing)» та ін.; – за цими й іншими тренінгами робоча група SANS проводить навчання і глобальну сертифікацію (Global Information Assurance Certification – GIAC) фахівців за різноманітними спеціальностями, зокрема: Аудитор систем і мереж (Systems and Network Auditor – GSNA); Сертифікований спеціаліст ISO-27000 (Certified ISO-27000 Specialist – G2700); Професіонал з інформаційної безпеки (Information Security Professional – GISP) та ін. Керівництва робочої групи ІТ-аудиту (IT Audit community): «Аудит відповідності внутрішньої політики критеріям QualysGuard та Центру інформаційної безпеки (Auditing for Policy Compliance with QualysGuard and CIS Benchmarks)»; «Вибір корпоративної системи миттєвого сповіщення та впровадження контролів аудиту (Choosing corporate level instant messaging system and implementing audit controls)» та ін. Керівництва (Checklists and Step-by-Step Guides), спільної ініціативи робочих груп SANS/GIAC та CIS, – Консенсусу щодо оцінювання зрілості операційної безпеки (Security Consensus Operational Readiness Evaluation – S.C.O.R.E.): «План системної безпеки (System Security Plan)»; «ІТ-етика (IT Ethics Handbook)» та ін. |
| Інститут розробки програмного забезпечення, при Університеті Карнегі-Меллон (Software Engineering Institute – SEI Carnegie Mellon University) | Методології (Methods): «Оцінювання операційно критичних загроз, активів та вразливостей (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM – OCTAVE®)» – набір інструментів, технік та методів для ризико-орієнтованого стратегічного оцінювання і планування інформаційної безпеки; «Розробка вимог щодо якості безпеки (The Security Quality Requirements Engineering – SQUARE)» – розроблена підрозділом SEI – CERT, методологія побудови безпеки на ранніх стадіях життєвого циклу розробки ПЗ та ін. Керівництва (Guides): «Впровадження методології OCTAVE (OCTAVE Method Implementation Guide)» та ін. Тренінги (SEI Trainings): «Основи застосування моделі еластичного менеджменту (Introduction to the CERT Resilience Management Model – RMM)» та ін. Моделі (Models): «Модель технологічної зрілості (Capability Maturity Model – CMMSM) – для оцінки та удосконалення бізнес-процесів організації; (Capability Maturity Model Integration – CMMI®)» – набір моделей зрілості для бізнес-процесів: закупівель, виробництва, послуг, персоналу та ін. |
| Організація «ITSq, LLC», США – створена за ініціативи Carnegie Mellon University | Моделі (Models) ІТ-аутсорсингу: «Модель використання можливостей для провайдерів ІТ-сервісів (eSourcing Capability Model for Service Providers – eSCM-SP)»; «Модель використання можливостей для клієнтів ІТ-сервісів (eSourcing Capability Model for Client Organizations – eSCM-CL)» |
| Міжнародний консорціум із сертифікації безпеки інформаційних систем (International Information Systems Security Certification Consortium – (ISC)I®) | Тренінгові курси та навчальні матеріали (Whitepapers, Case Studies): «Потреба у безпеці ПЗ (CSSLP Whitepaper I: The Need for Secure Software)»; «Охорона важливої інформації (Case Study: Securing the Right Information Security Team)» та ін. – за цими й іншими матеріалами організація проводить глобальну сертифікацію фахівців за спеціальностями: «Сертифікований професіонал з безпеки життєвого циклу ПЗ (Certified Secure Software Lifecycle Professional – CSSLP®)»; «Сертифікований професіонал з безпеки інформаційних систем (Certified Information Systems Security Professional – CISSP®)» та ін. Керівництва (Guides): «Визначення і виявлення походження загроз ((ISC)I eBook I: Identifying and Addressing Evolving Threats)»; «Офіційне керівництво (ISC)I® для фахівця CISSP® (Official (ISC)I® Guide to the CISSP® CBK®)» та ін. |
| Інститут проектного менеджменту (Project Management Institute – PMI), США | Керівництво «Система знань з проектного менеджменту (A Guide to the Project Management Body of Knowledge – PMBOK® Guide)» – методологія професійного управління проектами, заснована на найкращому світовому досвіді. Стандарти (Standards): «Модель зрілості проектного менеджменту організації (The Organizational Project Management Maturity Model – OPM3®)» та ін. |
| Організація «The Open Group's Architecture Forum», США | Керівництво «Концептуальна основа моделювання архітектури організації (The Open Group Architecture Framework – TOGAF®)» – пропонує холистичний підхід побудови інформаційної архітектури організації, із застосуванням різносторонніх методів проектування, планування, впровадження та управління |
| Організація «Tele Management Forum», США | Керівництва розробки прикладного ПЗ для телекомунікаційних організацій: «Нове покоління систем і ПЗ (New Generation Operation System and Software – NGOSS)»; «Технологічно нейтральна архітектура (Technology Neutral Architecture – TNA) та ін. Референтні моделі бізнес-процесів і прикладного ПЗ телекомунікаційної галузі: «Розширена карта телекомунікаційних операцій (enhanced Telecom Operations Map – eTOM®)»; «Карта телекомунікаційного ПЗ (Telecom Application Map – TAM)»; «Модель обміну даними й інформацією (Shared Information and Data Model – SID)» та ін. |
| Європейська фундація управління якістю (European Foundation for Quality Management – EFQM) | Модель «Створення конкурентних переваг (EFQM Excellence Model)» – пропонує холистичний підхід до управління організацією, а також методологію для самооцінки системи менеджменту та ін. |

| Корпорації | |
|--|---|
| Microsoft Inc. | Керівництва (Frameworks): «Концептуальна основа управління операціями (Microsoft Operations Framework – MOF)» – пропонує методологію створення в організації ефективного і надійного IT-середовища для досягнення цілей бізнесу; «Концептуальна основа управління рішеннями (Microsoft Solutions Framework – MSF)» – узгоджений набір концепцій, моделей і правил, заснованих на практичному досвіді та технологіях Microsoft, щодо розробки програмного забезпечення |
| Hewlett-Packard Inc. (HP) | Методологія «Сервіс-менеджменту IT (HP IT Service Delivery Framework – HP ITSM)» – пропонує референтну процесну модель побудови IT-підрозділу організації, орієнтовану на задоволення потреб клієнтів IT-послуг |
| International Business Machines Inc. (IBM) | Методологія «Управління ресурсами IT-інфраструктури (Infrastructure resource management – IRM)» – пропонує холістичну модель управління IT-ресурсами організації, із застосуванням методів різносторонньої оцінки й аналізу досягнення запланованих бізнес-цілей |
| Motorola, Inc. | Методологія «Шість сігма (Six Sigma™)» – спрямована на вдосконалення бізнес-процесів організації, підвищення їх якості та зниження нестабільності, шляхом виявлення та усунення причин дефектів (помилки) в операційній діяльності |
| Toyota Inc. | Методологія «Ощадливі IT (Lean IT)» – заснована на концепції управління виробничими втратами організації (Toyota Production System – Lean), клієнто-орієнтована методологія управління IT-середовищем, основна ідея якої полягає у вилученні із нього того, що є зайвим: ресурсів, процесів, інвестицій тощо, які не додають вартості продуктам чи послугам, що пропонуються клієнту |

Основою методології IT-аудиту за COBIT є застосування критеріїв і моделей зрілості для оцінювання ефективності і потенціалу процесів IT-середовища за визначеними контрольними об'єктами/цілями.

Застосування методології та інструментарію COBIT дозволяє IT-керівникам усунути недоліки IT-середовища організації з урахуванням вимог контролю, технічних питань і бізнес-ризиків, та донести досягнутий рівень контролю до відомо зацікавлених сторін. Методологія дає можливість розробляти чіткі політики IT-контролю в організаціях, керуючись найкращим досвідом у цій сфері.

Керівництво постійно вдосконалюється та гармонізується з іншими відомими стандартами і методологіями IT-менеджменту, зокрема ITIL. Публікацію 5-го видання COBIT, згідно з інформацією на офіційному сайті ISACA, заплановано на початок 2012 р. Це видання анонсовано як консолідацію та інтеграцію COBIT 4.1 з іншими ключовими керівництвами (методологіями) ITGI – ISACA: Val IT 2.0, Risk IT, BMIS, ITAF та ін. (табл. 3) в єдиний мета-стандарт методології IT Governance.

Методологічне забезпечення, розроблене іншими професійними аудиторськими організаціями, наприклад Асоціацією присяжних дипломованих бухгалтерів (ACCA) у Великобританії, Американським інститутом дипломованих громадських бухгалтерів (AICPA) у США та ін., стосується аудиту інформаційних технологій опосередковано. Оскільки більшість із них спеціалізуються у сфері фінансового аудиту і вдаються до застосування методів IT-аудиту, як правило, лише з метою висвітлення окремих аспектів, пов'язаних із застосуванням IT для надання додаткової впевненості і якості аудиторському висновку.

Велике значення у практиці аудиту інформаційних технологій відіграє методологічне забезпечення професійних організацій у сфері стандартів IT-менеджменту, наприклад таких, як SANS, SEI, PMI, (ISC)I та ін. (табл. 3). Таке забезпечення на відміну від методологій високого рівня, таких як COBIT (ITGI) і йому подібних, як правило, є більш вузькоспе-

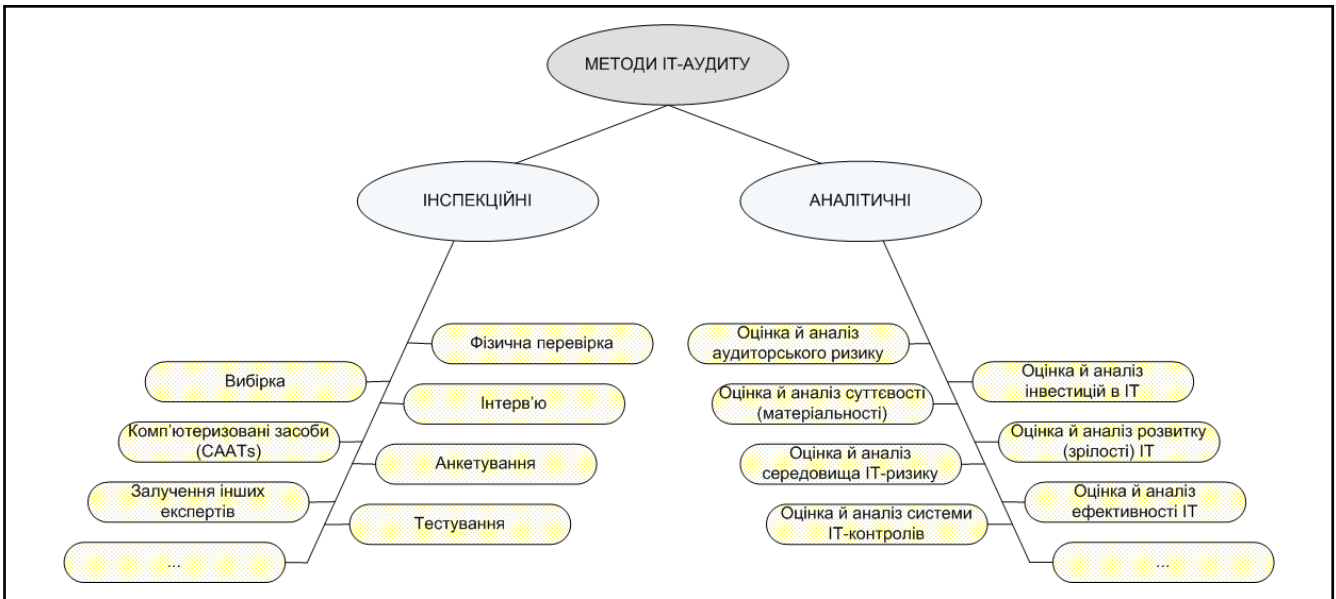
ціалізованим і охоплює найкращий досвід, моделі, керівні принципи і т.п. щодо окремих аспектів IT-менеджменту організації, які можуть бути застосовані у процесі IT-аудиту як еталони для порівняння.

Також не менш важливими для професійного методологічного забезпечення аудиту інформаційних технологій є методології IT-менеджменту, розроблені «великим бізнесом» – всесвітньовідомими корпораціями, наприклад такими, як Microsoft, HP, IBM та ін. (табл. 3). Особливість такого забезпечення полягає в тому, що воно засноване на багаторічному досвіді корпорацій у застосуванні інформаційних технологій для надскладних бізнес-систем.

В Україні методологічне забезпечення IT-аудиту професійного рівня практично не розробляється. Вітчизняні професійні об'єднання аудиторів здебільшого практикують навчання та сертифікацію фахівців у сфері бухгалтерського обліку і фінансової звітності за міжнародними програмами ACCA DipIFR, CAP/CIPA, CAPA, CAPS та ін. Зазначені програми якщо і розглядають окремі аспекти аудиту інформаційних технологій, то лише опосередковано, наскільки це необхідно для якісного і професійного проведення фінансового аудиту.

Тому нині як професійне методологічне забезпечення IT-аудиту в Україні застосовується відповідне забезпечення, розроблене професійними організаціями розвинених країн світу, зокрема керівництва і рекомендації IT Governance Institute, США.

Слід зазначити, що методологічне забезпечення аудиту інформаційних технологій, зрештою як і інших видів аудиту організацій, покликане надати його виконавцям загальні орієнтири/еталони (методологічні засади) здійснення такої діяльності на високоякісному професійному рівні, не пропонуючи і не нав'язуючи при цьому конкретні прикладні методи чи технології. Саме вони є основою методичного забезпечення аудиту інформаційних технологій (в деяких джерелах можна зустріти термін «внутрішні» або «внутріш-



Узагальнена класифікація методів аудиту інформаційних технологій

ньо-фірмові» стандарти [5, 10, 11]). Розробка методичного забезпечення зазвичай покладається на самих аудиторів.

Отже, під методичним забезпеченням аудиту інформаційних технологій будемо розуміти сукупність прикладних методів і технологій їх застосування (технік, методик тощо), розроблених аудиторами (аудиторськими організаціями) самостійно, або запозичених у практичному середовищі, для практичного виконання аудиторських процедур (заходів). Таке забезпечення не повинно суперечити законодавству, встановленим нормам міжнародного і національного методологічного забезпечення аудиторської діяльності, а також умовам договору із замовником аудиту.

Ключовим у цьому виді забезпечення є поняття методу ІТ-аудиту. Виходячи з аналізу різноманітних трактувань сутності терміну «метод аудиту» [10], а також керуючись відповідним методичним забезпеченням аудиту інформаційних технологій і найкращим світовим досвідом провідних аудиторських організацій у цій сфері [6, 12, 15–18], пропонуємо розуміти під методом ІТ-аудиту – сукупність конкретних дій, способів, прийомів, інструментів тощо, які застосовуються аудитором при виконанні тих або інших заходів ІТ-аудиту для досягнення мети його проведення.

Виходячи з аналізу різноманітних підходів до класифікації методів аудиту [10], а також керуючись найкращими світовими практиками (керівництвами, методологіями тощо) у сфері аудиту інформаційних технологій [12–20], пропонуємо всі методи ІТ-аудиту за призначенням і змістом розділити на два класи: інспекційні та аналітичні (див. рис.).

До інспекційних методів ІТ-аудиту пропонуємо відносити – методи, які застосовуються для здійснення збору необхідного і достатнього обсягу аудиторських доказів (фактів щодо поточного стану ІТ-середовища об'єкта аудиту й іншої інформації). Вони мають на меті забезпечити належний рівень об'єктивності і достовірності аудиторського висновку та рекомендацій.

До аналітичних методів ІТ-аудиту пропонуємо відносити – методи, які застосовуються для здійснення професійної оцінки й аналізу поточного стану ІТ-середовища організації, на підставі зібраних аудиторських доказів й іншої інформації. Вони мають на меті забезпечити аудиторський висновок та рекомендації необхідною і достатньою аналітичною інформацією (свідцтвами аудиту).

Нині використовувані на практиці інспекційні й аналітичні методи ІТ-аудиту є досить різноманітними [6, 12–20]. Вибір конкретного методу здійснюється виходячи із цілей, завдань й обмежень ІТ-аудиту тощо, поставлених замовником, а також рівня фахових знань і практичного досвіду аудитора.

Висновки

Для якісного проведення аудиту інформаційних технологій на високому професійному рівні велике значення має відповідне методологічне й методичне забезпечення.

Методологічне забезпечення міжнародного рівня нині практично охоплює всі аспекти здійснення ІТ-аудиту. Разом із цим, зважаючи на динаміку розвитку інформаційних технологій та їх вплив на діяльність організації, його постійний розвиток і удосконалення мають стати першочерговими завданнями міжнародних інституцій, що його розробляють.

На національному рівні найкращі досягнення у цій сфері мають США та Великобританія. Нормативні документи цього рівня конкретизують міжнародні і доповнюють їх у тих аспектах, що є важливими для кожної окремої держави, відповідно до стану розвитку ІТ-аудиту.

Професійний рівень нормативного забезпечення є найбільш розвиненим. Найвагомий внесок у його розвиток роблять професійні організації США у сфері аудиту і стандартів ІТ-менеджменту.

Необхідність розвитку методологічного й методичного забезпечення ІТ-аудиту в Україні обумовлює необхідність за-

позичення і використання найкращого світового досвіду у цій сфері, а також налагодження і розвитку співпраці відповідних інститутів у нашій державі із зарубіжними професійними організаціями на всіх рівнях (міжнародному, національному, професійному).

Література

1. Про аудиторську діяльність: Закон України 22.04.93 р. №2939-VI (редакція від 26.05.2011 р.). [Електронний ресурс] / Верховна Рада України [сайт] – Режим доступу до закону: <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3125-12&c=1#Current>. – Назва з екрану.
2. Про затвердження Концептуальної основи контролю аудиторської діяльності в Україні: Рішення Аудиторської палати України від 27.09.2007 р. №182/3. [Електронний ресурс] / Аудиторська палата України [сайт] – Режим доступу до рішення: <http://apu.com.ua/files/ris/946583183.doc>
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. Міжнародне співробітництво. [Електронний ресурс] / Рахункова палата України [сайт] – Режим доступу: http://www.asrda.gov.ua/control/main/uk/publish/printable_article/1377824
5. Глущенко В.В., Риженко І.Є. Правове регулювання та методичне забезпечення аудиторської діяльності в Україні. [Електронний ресурс] – Режим доступу: http://www.nbu.gov.ua/portal/Soc_Gum/Fkd/2009_1/R2/1.pdf

6. Лазарева С.Ф., Ус Р.Л. Сучасні методи аудиту інформаційних технологій // Держава та регіони: науково-виробничий журнал, вип. 4. – Запоріжжя, 2011. – С. 29–35.
7. Новіченко В.М. Аудит: Історія. Розвиток. Майбутнє. [Електронний ресурс] – Режим доступу: <http://apu.com.ua/files/pub/2132130153.doc>
8. Макеєва О. Нагляд за професією аудитора в Україні – чи не час переймати досвід? [Електронний ресурс] – Режим доступу: <http://apu.com.ua/files/pub/194372796.doc>
9. Макеєва О. Конгрес аудиторів Німеччини. [Електронний ресурс] – Режим доступу: <http://apu.com.ua/files/pub/1103551316.doc>
10. Рудницький В.С. Методологія і організація аудиту. – Тернопіль: «Економічна думка», 1998. – 196 с.
11. Усач Б.Ф., Душко З.О., Колос М.М. Організація і методика аудиту: Підручник. – К.: Знання, 2006. – 295 с.
12. COBIT 4.1 // IT Governance Institute, 2007. – 196 p.
13. Enterprise Value: Governance of IT Investments – The Val IT Framework 2.0 // IT Governance Institute, 2008. – 119 p.
14. Information technology – Security techniques – Information security risk management – BS ISO/IEC 27005:2008 // BSI, 2008. – 64 p.
15. ITIL v.3 – Lifecycle Publication Suite // OGC, 2007. – 1200 p.
16. Introduction to IT Audit Student Notes // INTOSAI, 2007. – 45 p.
17. IT Methods Student Notes // INTOSAI, 2007. – 97 p.
18. IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals // ISACA, 2010. – 330 p.
19. The Business Model for Information Security // ISACA, 2010 – 73 p.
20. The Risk IT Framework // ISACA, 2009. – 107 p.

В.В. ЧЕПКА,

к.е.н., доцент, Київський національний економічний університет ім. В. Гетьмана

Кооперативні об'єднання у сільському господарстві: функціонування та фінансування

Статтю присвячено дослідженню розвитку кооперативних об'єднань на основі малих та середніх аграрних підприємств та створенню дієвої моделі кредитної кооперації в сільському господарстві.

Ключові слова: сільськогосподарські кооперативи, кредитна кооперація, спеціалізовані кредитні установи.

Статья посвящена исследованию развития кооперативных объединений на основе малых и средних аграрных предприятий и созданию действенной модели кредитной кооперации в сельском хозяйстве.

Ключевые слова: сельскохозяйственные кооперативы, кредитная кооперация, специализированные кредитные учреждения.

The article is devoted research of development of co-operative associations on the base of small and middle agrarian enterprises and creation of effective model of credit co-operation in agriculture.

Keywords: agricultural cooperative stores, credit co-operation, credit establishments are specialized.

Постановка проблеми. Необхідність функціонування кооперативних об'єднань на основі малих та середніх аграрних підприємств зумовлена нагальною потребою у розбудові заготівельної, переробної, допоміжної, обслуговуючої та кредитної інфраструктури в сільському господарстві. Досвід функціонування такої розгалуженої виробничої та обслуговуючої інфраструктури в розвинених країнах світу засвідчує, що за-