Ус Р.Л., асистент кафедри інформаційного менеджменту ДВНЗ “Київський національний економічний університет імені Вадима Гетьмана”
Адреса: м. Київ, вул. Проспект Перемоги 54/1
Тел.: 050-97-57-984

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ АУДИТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

АНОТАЦІЯ. *Досліджено стан зарубіжного і вітчизняного нормативно-правового забезпечення аудиту інформаційних технологій, запропоновано модель системи такого забезпечення. Надано пропозиції щодо його вдосконалення і застосування в Україні.*

КЛЮЧОВІ СЛОВА. *ІТ-аудит, нормативно-правове забезпечення ІТ-аудиту, Закон Сарбейнса-Окслі.*

АННОТАЦИЯ. *Исследовано состояние зарубежного и отечественного нормативно-правового обеспечения аудита информационных технологий, предложено модель системы такого обеспечения. Приведены предложения его усовершенствования и использования в Украине.*

КЛЮЧЕВЫЕ СЛОВА. *ИТ-аудит, нормативно-правовое обеспечение ИТ-аудита, Закон Сарбейнса-Оксли.*

ANNOTATION. *Investigated the state of the foreign and native regulatory and legal framework for the information technology audit, proposed the model of the system of this. Attached the propositions about improvement and use of the regulatory and legal framework for the information technology audit in Ukraine.*

KEY WORDS. *IT-audit, IT-audit regulatory and legal framework, Sarbanes-Oxley Act (SOX).*

Постановка проблеми. Сучасним ефективним інструментом інформаційного менеджменту організацій, який набуває дедалі більшого значення і застосування є аудит інформаційних технологій (ІТ-аудит). Він поєднує багатовіковий досвід, методологічні засади, методичні прийоми і нормативно-правове забезпечення аудиторської діяльності з найкращими практиками і стандартами в галузі управління ІТ. Застосування ІТ-аудиту в системі управління економічними об’єктами, зазвичай, має на меті підвищити продуктивність, ефективність й економічність функціонування інформаційних технологій, збільшити переваги і зменшити недоліки від їх

використання для досягнення цілей бізнесу, а також обґрунтувати відповідні інвестиції тощо. Запорукою належного (якісного), професійного, і, що не менш важливо, правомірного проведення ІТ-аудиту, як і будь-якого іншого виду аудиту організацій, є застосування його виконавцями відповідного нормативно-правового забезпечення.

Метою статті є дослідження стану зарубіжного і вітчизняного нормативно-правового забезпечення аудиту інформаційних технологій, та надання пропозицій щодо його вдосконалення і застосування в Україні.

Виклад основного матеріалу. Керуючись (вітчизняними і зарубіжними) науковими, практичними та правовими джерелами [1-14], під нормативно-правовим забезпеченням ІТ-аудиту будемо розуміти чинні у державі закони, міждержавні і міжнародні угоди про співпрацю, нормативно-правові акти, положення, інструкції, директиви тощо, які визначають правові засади здійснення такої діяльності, зокрема права, обов'язки, відповідальність у взаємовідносинах сторін (фізичних та юридичних осіб) між собою та з державними органами, а також регламентують її здійснення у правовому полі.

У зв'язку з тим, що аудит інформаційних технологій є одним із видів аудиту організацій [8], пропонуємо виділити чотири рівня його нормативно-правового забезпечення. Розглянемо їх детальніше.

До ***першого рівня*** слід віднести нормативно-правові документи, які визначають суть і загальні правові засади здійснення аудиторської діяльності. Основним із них у кожній країні, де легалізовано таку діяльність, є *закон про аудит* або його аналоги. Його призначення полягає у визначенні суті, суб'єктів, об'єктів і напрямків аудиту; прав, обов'язків і відповідальності суб'єктів аудиторської діяльності; порядку сертифікації аудиторів, створення їх громадських організацій, а також створення і функціонування вищих органів державного регулювання та професійного контролю такої діяльності тощо. Уперше такий закон було прийнято у Великобританії у 1844 р. Згодом, аналогічні закони були прийняті у Франції – 1867р., США – 1887 р. (за іншими джерелами у 1937 р.), Швеції – 1895 р., Німеччині – 1931 р. й інших країнах.

Зарубіжний досвід свідчить про те, що аудит є обов'язковим атрибутом ринкової економіки будь-якої країни [9]. У зв'язку з тим, що в Україні ринкові відносини стали формуватись значно пізніше ніж у країнах Заходу, то Закон «Про аудиторську діяльність» у нашій державі було прийнято у 1993 р. В інших країнах СНД аудит також розвивається у міру формування засад ринкової економіки,

виникнення підприємств недержавної форми власності, приватизації державного майна тощо. Зокрема, у Росії закон про аудит було прийнято лише у 2001 р. [1, 9].

Нині, перша редакція Закону України «Про аудиторську діяльність» від 22.04.1993 р. зазнала ряду змін і доповнень [1, 2]. В останній його редакції (від 26.05.2011 р.) значно розширено правові засади здійснення аудиторської діяльності в Україні, а також закладено підґрунтя і перспективи для створення спеціалізованого нормативно-правового забезпечення для усіх відомих нині і таких, що будуть виникати у майбутньому, видів аудиту, у тому числі аудиту інформаційних технологій. Зокрема, у Статті 2 Закону допускається здійснення, окрім фінансового аудиту, також й інших видів аудиторської діяльності, що повинні регулюватися спеціальним законодавством. У Статті 3 Закону зазначено, що окрім аудиту (як фінансового контролю організацій), аудитори (аудиторські фірми) можуть надавати й інші аудиторські послуги, пов'язані з їх професійною діяльністю, перелік яких визначається Аудиторською палатою України відповідно до стандартів аудиту.

Чинний «Перелік послуг, які можуть надавати аудитори (аудиторські фірми)» затверджено Рішенням № 182/5 Аудиторської палати України від 27.09.2007 р. Серед зазначених у ньому видів послуг, пов’язані з IT-аудитом представлені у групах: «Завдання з надання впевненості» та «Інші послуги, пов’язані з професійною діяльністю аудиторів (аудиторських фірм), визначені Законом України «Про аудиторську діяльність».

Зокрема, у групі *«Завдання з надання впевненості»* послугами, що мають пряме або опосередковане відношення до IT-аудиту, є такі: оцінка (перевірка) ефективності (відповідності) системи внутрішнього контролю (аудиту); оцінка (перевірка) ефективності (відповідності) інформаційних систем (технологій); оцінка (перевірка) ефективності систем інформаційної безпеки діяльності підприємств».

У групі *«Інші послуги, пов’язані з професійною діяльністю аудиторів (аудиторських фірм), визначені Законом України «Про аудиторську діяльність»* до таких послуг відносяться: консультації з питань системи внутрішнього контролю; консультації з питань застосування інформаційних технологій; консультації з інших питань управління та ведення бізнесу, зокрема, консультування з питань вибору програмних продуктів або технічної бази з автоматизації обліку та внутрішнього контролю (аудиту), розробка схем документообороту, форм внутрішніх документів і напрямів інформаційних потоків у системі управління; проведення тренінгів, семінарів з питань обліку, оподаткування, правового забезпечення та організації управління, безпеки бізнесу тощо.

До ***другого рівня*** нормативно-правового забезпечення IT-аудиту пропонуємо відносити закони, директиви, постанови, укази, інструкції, рішення та інші нормативно-правові акти, які додатково роз'яснюють і конкретизують (деталізують) окремі аспекти проведення аудиту, зокрема у спеціальних, підконтрольних державі (особливих) видах економічної діяльності, наприклад, у сфері фондового ринку, банківської справи, страхування та ін.

Ініціаторами таких документів, як правило, виступають різноманітні урядові установи. Наприклад, у США: Комісія з цінних паперів і фондового ринку (US Securities Exchange Commission - SEC), Головне бюджетно-контрольне управління (US General Accounting Office - GAO) та ін.; в Україні: Кабінет Міністрів, Секретаріат Президента, Аудиторська палата України, окремі міністерства і відомства та ін.

Зокрема у США, на цьому рівні нормативно-правового забезпечення аудиту, було прийнято ряд важливих законів й інших нормативних документів, які, залежно від їх цільового застосування, окремими положеннями звертаються до потреби правового регулювання і контролю впливу використання інформаційних технологій державними та комерційними організаціями на результати їх діяльності, а також аудиту відповідно. Деякі із цих документів нині застосовуються у практичному середовищі IT-аудиту, у якості правового обґрунтування здійснення такої діяльності (див. табл. 1) [4-6, 12, 14].

У світовій практиці найбільш відомим із них є *Закон «Сарбейнса-Окслі (The Sarbanes-Oxley Act – SOX)»*. Його прийняття у 2002 р. було реакцією уряду США на всесвітньо відомі скандали 2001-2002 рр., пов'язані з фінансовими махінаціями менеджменту корпорацій Enron, Tyco International, Adelphia, Peregrine Systems та WorldCom, у змові із зовнішніми аудиторами, які їх обслуговували. Такі події спричинили великі збитки не лише для бізнесу, а й для економіки США в цілому. Статті SOX висувають ряд жорстких вимог як до корпоративного менеджменту, так і до зовнішнього аудиту, зокрема щодо корпоративної відповідальності, аудиторської незалежності, прозорості фінансових транзакцій, складання звітності тощо. З них найбільш важливою для нормативно-правового забезпечення практики IT-аудиту є Стаття 404 «Оцінка системи внутрішнього контролю (Management Assessment of Internal Controls)», яка вимагає від менеджменту корпорацій проводити обов'язковий зовнішній аудит їх системи і процедур внутрішнього контролю перед підготовкою щорічної фінансової звітності.

Таблиця 1 – Нормативно-правові документи США, які застосовуються в якості правових засад аудиту інформаційних технологій

Нормативний документ	Застосування
Закон «Сарбейнса-Оклі» (The Sarbanes-Oxley Act – SOX), 2002 р.	Посилив державне регулювання і контроль господарської діяльності «великого бізнесу» (акціонерних товариств) США, а також аудиторських організацій. Визначив особисту відповідальність менеджменту корпорацій і зовнішніх аудиторів за банкрутства, спричинені їхніми неналежними або незаконними діями. Наклав жорсткі вимоги щодо підготовки фінансової та аудиторської звітності, а також зобов'язав менеджмент корпорацій, окрім щорічного фінансового аудиту, проводити також оцінку ефективності системи внутрішнього контролю (IT-систем, які зберігають й обробляють фінансові дані).
Закон «Гремма-Ліча-Блайлі» (The Gramm-Leach-Bliley Act – GLBA), 1999 р.	Стосується сфери фінансів, а саме комерційних банків, інвестиційних банків, страхових компаній, фондових бірж і організацій, які займаються торгівлею цінними паперами. Визначає певні стандарти конфіденційності персональної інформації клієнтів таких установ, і зобов'язує організації проектувати, впроваджувати і забезпечувати достатні контролі для її захисту.
«Кодекс федеральних інструкцій» США, Розділ 21 – Стаття 11 (Title 21 CFR Part 11 of the Code of Federal Regulations), 1997 р.	Взаємодіє з керівництвами Управління у сфері харчування і медикаментів США (Food and Drug Administration - FDA) стосовно питань електронних записів і електронного підпису. У Статті 11 визначаються критерії, за якими електронні записи і електронний підпис вважаються достовірними, надійними і еквівалентними фізичним (на паперових носіях).
Закон «Клінгера-Коена» (Clinger-Cohen Act – CCA), 1996 р.	Зобов'язав усі федеральні агентства США фокусуватися на результатах, яких вони досягають, інвестуючи в інформаційні технології. Вимагає від керівництва кожного агентства побудови процесів, які б гарантували максимізацію віддачі і мінімізацію ризиків від використання IT. Зокрема, цей акт зробив посаду IT-директора (Chief Information Officer - CIO) обов'язковою для державних організацій США і визначив сферу їх відповідальності.
Закон «Про портативність і підзвітність страхування здоров'я» (The Health Insurance Portability and Accountability Act – HIPAA), 1996 р.	Стосується галузі медичного обслуговування США (медичних послуг, медичного страхування та ін.). У його другій частині висувається вимога до опублікування національних стандартів щодо інформаційної безпеки операцій з електронними даними стосовно пацієнтів медичних закладів. Ці стандарти покликані забезпечити достатній рівень захисту інформації про пацієнтів, особливо при їх передачі в електронних системах управління захисту здоров'я США.
Закон «Про практику зовнішньої корупції» (The Foreign Corrupt Practices Act – FCPA), 1977 р.	Відомий, у першу чергу, за його двома головними положеннями, одне з яких скеровує контроль за виконанням вимог щодо прозорості і незалежності аудиту до SEC, а інше стосується корупції серед зовнішніх чиновників.

У Статті 404 SOX зазначається, що менеджмент організації несе особисту відповідальність за впровадження і підтримку ефективної системи та процедур внутрішнього контролю, і що завданням зовнішнього аудиту є оцінка рівня їх ефективності, надійності і достатності для формування незалежної думки стосовно достовірності інформації, поданої у фінансовій звітності. При цьому, оцінка системи і

процедур внутрішнього контролю передбачає комплексну перевірку контролів IT-середовища організації (інформаційних систем, IT-процесів, IT-ризиків тощо).

Прийняття Закону SOX мало вагомий вплив на практику аудиту в США в цілому, оскільки ним було ініційовано створення «Наглядової ради за веденням фінансової звітності публічних компаній (Public Company Accounting Oversight Board - PCAOB)», з метою контролю, регулювання, перевірки та застосування дисциплінарних заходів до аудиторських організацій, які діють в якості аудиторів публічних організацій. Цим було скасовано, існуючу до цього, саморегульованість аудиторської діяльності у США.

Вимоги SOX поширюються не лише на американські акціонерні товариства, але також на: іноземні корпорації, які проходять лістинг на біржах США; іноземні організації, чия діяльність чинить значний вплив на американські організації, які проходять лістинг на біржах США; іноземні організації, які мають (або планують) ділові зв’язки з урядовими організаціями США; іноземні організації зі значним об’ємом операцій на території США; іноземні організації, які планують процес злиття або поглинання з організацією, яка проходить лістинг на біржах США; а також на філіали американських організацій за кордоном. Дія закону не розповсюджується на приватні підприємства.

В аудиторській практиці Великобританії застосовуються нормативні документами схожі за змістом і застосуванням із Законом США SOX. Найбільш відомим із них є «Комбінований кодекс принципів належного управління і кодекс найкращого досвіду (The combined code Principles of good governance and code of best practice)». Він висуває до акціонерних товариств, які проходять лістинг на Лондонській фондовій біржі (London Stock Exchange), і до зовнішніх аудиторів схожі із Законом «Сарбейнса-Окслі» вимоги, зокрема щодо необхідності проведення аудиту системи і процедур внутрішнього контролю корпорацій [13].

У Південно-Африканській Республіці для схожих із SOX цілей застосовують серію нормативних документів King (I, II, III). На вимогу уряду цієї країни, з липня 2010 р. акціонерні товариства, які проходять лістинг на Йоганнесбургській фондовій біржі у Південно-Африканській Республіці (South Africa's JSE Securities Exchange), повинні виконувати вимоги «Кодексу принципів управління Південно-Африканської Республіки (Code of Governance Principles for South Africa - King III)», які є схожими із тими, що висуваються у Законі «Сарбейнса-Окслі». Додатково, King III рекомендує менеджменту корпорацій складати фінансову звітність у відповідності із керівними

принципами «Глобальної звітної ініціативи (Global Reporting Initiative's Sustainability Reporting Guidelines)» [11].

Інші розвинені країни світу, такі як Канада, Австралія, Японія і країни-члени Європейського Союзу (ЄС) теж мають ряд законів й інших нормативно-правових документів на рівні спеціального регулювання аудиторської діяльності, які схожі за змістом і застосуванням із тими, що діють у США [6, 12].

В Україні, на відміну від найбільш розвинених країн світу, нормативно-правове забезпечення аудиту спеціального призначення може бути застосоване лише для опосередкованого правового обґрунтування тих або інших заходів ІТ-аудиту. До їх числа можна віднести (див. табл. 2) [3]:

Таблиця 2 – Спеціальне нормативно-правове забезпечення аудиторської діяльності в Україні

Тип документів	Назва документів
Закони України	«Про акціонерні товариства» від 17.09.2008 р. № 514-VI; «Про цінні папери та фондовий ринок» від 23.02.2006 р. № 3480-IV; «Про банки і банківську діяльність» від 16.06.2000 р. № 2121-III; «Про бухгалтерський облік та фінансову звітність» від 16.07.1999 р. № 996-XIV; «Про страхування» від 07.03.1996 р. № 85/96-ВР; «Про господарські товариства» від 19.09.1991 р. № 1576-XII та ін.
Підзаконні нормативні акти	Рішення ДКЦПФР «Про затвердження Положення щодо підготовки аудиторських висновків, які подаються до Державної комісії з цінних паперів та фондового ринку при розкритті інформації емітентами та професійними учасниками фондового ринку» від 19.12.2006 р. № 1528; Розпорядження Держфінпослуг України «Про затвердження Порядку ведення реєстру аудиторів, які можуть проводити аудиторські перевірки фінансових установ» від 19.02.2004 р. № 86; Постанова Правління НБУ «Про затвердження Положення про організацію бухгалтерського обліку та звітності в банках України» від 30.12.1998 р. № 566; Наказ Фонду державного майна України «Про затвердження Методичних роз'яснень стосовно здійснення аудиторських перевірок фінансового стану підприємств, що приватизуються» від 03.08.1995 р. № 998 та ін.
Нормативні акти Аудиторської палати України	«Методичні рекомендації аудиторам на випадок залучення їх до процесуальних дій в якості свідків, експертів або спеціалістів»; «Концептуальна основа контролю аудиторської діяльності в Україні»; «Перелік послуг, які можуть надавати аудитори (аудиторські фірми)» та ін.

До ***третього рівня*** нормативно-правового забезпечення ІТ-аудиту пропонуємо відносити нормативні документами, які визначають правові засади державного регулювання діяльності фізичних і юридичних осіб та їх взаємодії з державними органами у сфері інформації (інформаційних ресурсів, інформаційних систем і технологій, інформатизації суспільства, міжнародної і міждержавної співпраці у сфері інформаційної безпеки й охорони стратегічної, секретної інформації тощо). Такі нормативні документи є досить різними у кожній країні. Наприклад, у США відомими нормативними документами у сфері інформації є: Закон «Про

конфіденційність 1974 р. (Privacy Act of 1974)»; Закон «Про захист он-лайн конфіденційності дітей (Children's Online Privacy Protection – COPPA)», 1998 р.; Закон «Про захист персональної інформації та електронних документів (Personal Information Protection and Electronic Documents Act - PIPEDA)», 2000 р.; Закон «Про електронний уряд (The E-Government Act)», 2002 р.; Закон «Про управління федеральною інформаційною безпекою (The Federal Information Security Management Act of 2002 - FISMA)», 2002 р.; Закон «Про інформаційні технології для економічного і клінічного благополуччя (The Health Information Technology for Economic and Clinical Health Act – HITECH)», 2009 р.; «Стандарт захисту інформації в індустрії платіжних карт» (The Payment Card Industry Data Security Standard - PCI DSS – 2004 р., PCI DSS v. 2.0 – 2010 р.) та ін. [5, 6, 12, 14].

В Європейському Союзі державне регулювання в інформаційній сфері ґрунтується, в основному, на директивах Європарламенту і Ради Європи: «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних (Directive 95/46/EC)», 1995 р.; «Про правовий захист баз даних (Directive 96/9/ЄС)», 1996 р.; «Стосовно обробки персональних даних і захисту конфіденційності у телекомунікаційному секторі (Directive 97/66/EC)», 1997 р.; «Про певні правові аспекти електронної комерції на внутрішньому ринку (Directive COM (1998) 586 final)», 1998 р.; «Про конфіденційність та електронні комунікації (Directive 2002/58/EC)», 2002 р. тощо, а також на «Конвенції про кіберзлочинність (Convention on Cybercrime)», 2001 р. й інших нормативних документах [5, 6]. Їхні положення мають регулятивний характер як на рівні застосування державами-членами Європейського Союзу, так і на рівні міждержавної взаємодії з іншими країнами, зокрема щодо конфіденційності приватної і комерційної інформації, безпеки її переміщення каналами передачі даних тощо.

У вітчизняному законодавстві також прийнято ряд нормативних документів, які регулюють діяльність у сфері інформації. Наведемо основні з них (див. табл. 3):

Таблиця 3 – Нормативно-правове забезпечення діяльності в інформаційній сфері України

Тип документів	Назва документів
Закони України	«Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI; «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 р. № 3475-IV; «Про телекомунікації» від 18.11.2003 р. № 1280-IV; «Про Національну систему конфіденційного зв'язку» від 10.01.2002 р. № 2919-III; «Про Національну програму інформатизації» від 04.02.1998 р. № 74/98-ВР; «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 80/94-ВР; «Про науково-технічну інформацію» від 25.06.1993 р. № 3322-XII; «Про інформацію» від 02.10.1992 р. № 2657-XII та ін.
Підзаконні нормативні акти	Наказ Держспецзв'язку України «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 04.07.2008 р. № 112; Наказ Держспецзв'язку України «Про затвердження Положення про державний контроль за станом технічного захисту інформації» від 16.05.2007 р. № 87; Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 р. № 373 та ін.
Міжнародне Законодавство Співдружності незалежних держав (СНД)	«Модельний закон про захист дітей від інформації, яка шкодить їх здоров'ю та розвитку» від 03.12.2009 р.; «Модельний інформаційний кодекс для країн-учасниць СНД» від 03.04.2008 р.; «Модельний закон про інформатизацію, інформацію та захист інформації» від 18.11.2005 р. та ін.
Міжнародні Угоди	«Угода між Кабінетом Міністрів України та Урядом Демократичної Соціалістичної Республіки Шрі-Ланка про взаємну охорону секретної інформації» від 30.06.2010 р.; «Угода між Кабінетом Міністрів України та Урядом Республіки Македонія про взаємну охорону інформації з обмеженим доступом» від 29.06.2009 р.; «Угода між Кабінетом Міністрів України та Урядом Латвійської Республіки про співробітництво в області інформатизації» від 27.04.2006 р.; «Угода між Україною та Європейським Союзом про процедури безпеки, які стосуються обміну інформацією з обмеженим доступом» від 13.06.2005 р.; «Угода про співпрацю країн-учасниць Співдружності незалежних держав у боротьбі зі злочинами у сфері комп'ютерної інформації» від 01.06.2001 р. та ін.

До ***четвертого рівня*** нормативно-правового забезпечення аудиту інформаційних технологій пропонуємо відносити нормативні документи, які визначають суть і правові засади здійснення безпосередньо цього виду аудиторської діяльності (ІТ-аудиту), а також роз'яснюють окремі аспекти його проведення.

У світовій практиці поки не існує нормативно-правового забезпечення для безпосереднього регулювання діяльності у сфері ІТ-аудиту, однак у найбільш розвинених країнах світу нині розглядаються і підтримуються ініціативи щодо його розробки і застосування. Наприклад, сучасні державні програми США розглядають аудит інформаційних технологій як перспективний засіб досягнення тотального захисту «кібер-простору» (cyberspace) країни від будь-яких можливих загроз. Одна із таких програм – «Навчання мас (Educating the Masses)» передбачає впровадження у

навчальний процес студентів вищих навчальних закладів Сполучених Штатів вивчення аудиту і контролю інформаційних технологій та методик його проведення щодо безпеки, ефективності, продуктивності IT тощо [10].

Висновки

Дослідження стану нормативно-правового забезпечення аудиту інформаційних технологій у цілому показало, що перший рівень такого забезпечення – достатній у більшості країн, у яких легалізовано аудиторську діяльність. Другий рівень – найбільш повно, у порівнянні з іншими розвиненими країнами, представлений у США, тому їх досвід вартий наслідування. Третій рівень – умовно достатньо представлений у більшості країн, у тому числі в Україні, але потребує постійного вдосконалення, у зв'язку із динамічним розвитком інформаційних технологій. Четвертий рівень – практично не представлений у світовій практиці.

Специфіка IT-аудиту, яка суттєво відрізняє його від інших видів аудиту організацій (зокрема, за метою, цілями, об'єктами, заходами тощо), обумовлює потребу створення та впровадження спеціалізованих нормативних документів для визначення сутності і безпосереднього регулювання його практики. Це вимагає активних заходів державної політики, наприклад, налагодження співпраці з такими міжнародними організаціями як Асоціація аудиту і контролю інформаційних систем (Information Systems Audit and Control Association - ISACA), Інститут внутрішніх аудиторів (The Institute of Internal Auditors - IIA) та ін., а також професійними організаціями як Інститут стратегічного управління інформаційними технологіями (IT Governance Institute - ITGI), Інститут системних адміністраторів, аудиторів, спеціалістів у комп'ютерних мережах та інформаційній безпеці (SANS - SysAdmin, Audit, Network, Security Institute) та ін. Також важливою є державна підтримка створення і впровадження програм навчання з аудиту інформаційних технологій у вищих начальних закладах, і програм навчання та професійної сертифікації фахівців з IT-аудиту тощо.

Література

1. Про аудиторську діяльність: Закон України 22.04.1993 р. № 2939-VI (редакція від 22.04.1993 р.) [Електронний ресурс] / Верховна Рада України [сайт] – Режим доступу до закону.: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3125-12&ed=19930422&c=1#Current. – Назва з екрану.

2. Про аудиторську діяльність: Закон України 22.04.1993 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.

3. Нормативні акти, що регулюють аудиторську діяльність. [Електронний ресурс] / Аудиторська палата України [сайт] – Режим доступу до закону.: http://www.apu.com.ua/content.php?lang=ukr&c=page.php&id=0. – Назва з екрану.

4. Белоус С. Использование COBIT и ITIL для соответствия требованиям Закона Sarbanes-Oxley (SOX). [Електронний ресурс] – Режим доступу: http://www.itsmportal.com.ua/art001.html.

5. Василенко Д.П., студ., Маслак В.І., к.і.н., доц. Законодавство провідних країн світу в сфері захисту інформації УДК 342.7:002(100) // Вісник КДУ імені Михайла Остроградського, вип. 2/2010 (61), частина 1. – 2010 р. - С.128-132.

6. Климчук С. Загальна характеристика законодавства про інформаційну безпеку ЄС, США та Канади. // «Юридичний Журнал» №11, 2006 р. - [Електронний ресурс] – Режим доступу: http://justinian.com.ua/magazine.php?id=76.

7. Суть аудиту. Історичні аспекти становлення і розвитку аудиту. [Електронний ресурс] – Режим доступу: http://library.if.ua/books/78.html.

8. Ус Р.Л. Аудит інформаційних технологій як складова системи аудиту організацій // Формування ринкових відносин в Україні: збірник наукових праць, вип. 1 (116) / Наук. ред. І.Г. Манцуров. – К., 2011 р. – С. 163-168.

9. Усач Б.Ф., Душко З.О., Колос М.М. Організація і методика аудиту: Підручник. – К.: Знання, 2006. – 295 с.

10. Frederick Gallegos. Educating the Masses: Audit, Control and Security of Information Systems Today and Tomorrow // Information Systems Control Journal, ISACA., volume 6. 2004. - 3 p.

11. King III. [Електронний ресурс] – Режим доступу: http://en.wikipedia.org/wiki/King_III.

12. W. Scott Blackmer. Information Governance. [Електронний ресурс] – Режим доступу: http://www.infolawgroup.com/2010/05/articles/privacy-law/information-governance.

13. The combined code principles of good governance and code of best practice. Committee on Corporate Governance. 1998 – 2000. – 14 p.

14. Tommie W. Singleton. IT and Privacy Audits // ISACA JOURNAL, volume 5. 2009. - 4 p.