**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

# МОДЕЛІ ХОЛІСТИЧНОГО АУДИТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

АНОТАЦІЯ. *Стаття присвячена аудиту інформаційних технологій. Обґрунтовано об’єктивну необхідність дослідження середовища інформаційних технологій організації як складної системи. Виділено ключові підсистеми типового середовища інформаційних технологій організації, виявлено взаємозв’язки між ними, визначено середовище їх функціонування і взаємодії. Запропоновано структурну модель аудиту інформаційних технологій із застосуванням холістичного підходу, а також організаційні моделі аудитів її складових.*

КЛЮЧОВІ СЛОВА. *IT-аудит, аудит IT-інфраструктури, аудит IT-підрозділу, аудит IT-безпеки, IT-середовище, IT-ризик, IT-контроль, системний підхід, холістичний підхід, синергія.*

АННОТАЦИЯ. *Статья посвящена аудиту информационных технологий. Обоснована объективная необходимость исследования среды информационных технологий организации как сложной системы. Определены ключевые подсистемы типичной среды информационных технологий организации, определены взаимосвязи между ними, а также среда их функционирования и взаимодействия. Предложена структурная модель аудита информационных технологий с применением холистического подхода, а также организационные модели аудитов её составляющих.*

КЛЮЧЕВЫЕ СЛОВА. *ИТ-аудит, аудит ИТ-инфраструктуры, аудит ИТ-подразделения, аудит ИТ-безопасности, ИТ-среда, ИТ-риск, ИТ-контроль, системный подход, холистический подход, синергия.*

ANNOTATION. *Article is dedicated to information technology audit. Grounded an objective necessity of the information technology environment investigation as a complex system. Defined key subsystems of the typical information technology environment, identified interrelations among them, and their functioning and interaction environment. Proposed the structural model of the information technology audit based on the holistic approach, and organizational models of its components audit.*

KEY WORDS. *IT-audit, IT-infrastructure audit, IT-department audit, IT-security audit, IT-environment, IT-risk, IT-control, system approach, holistic approach, synergy.*

***Постановка проблеми.*** Постійний розвиток і ускладнення інформаційних технологій (ІТ), а також поглиблення їхньої інтеграції у господарські процеси організацій стимулюють потребу останніх у застосуванні нових ефективних засобів інформаційного менеджменту. Одним із таких засобів є **аудит інформаційних технологій (ІТ-аудит)**. Він поєднує багатовіковий досвід, методичні засади і нормативне забезпечення аудиту з кращими практиками і стандартами в галузі управління ІТ, та є ефективним засобом оцінки й аналізу ІТ-середовища. Його головне завдання – перетворити інформаційні технології в інструмент досягнення бізнес-цілей організації, а також у спосіб отримання додаткових конкурентних переваг. Однак, досягти цього стає дедалі важче, застосовуючи лише відомі нині часткові (функціонально-орієнтовані) види ІТ-аудиту, оскільки середовище інформаційних технологій сучасних організацій усе частіше представляє собою складну систему [1-6], і потребує застосування відповідного бачення, підходів, принципів і методів до організації та проведення аудиту.

***Метою статті*** є обґрунтування об'єктивної необхідності застосування холістичного підходу для дослідження середовища інформаційних технологій організації як складної системи, розробка структурної моделі аудиту інформаційних технологій, що реалізує цей підхід, а також організаційних моделей аудиту її складових.

***Виклад основного матеріалу.*** Нині дедалі більше теоретичних і прикладних досліджень у різноманітних галузях науки ґрунтуються на системному баченні (системному підході – *systems thinking, system approach*). Це зумовлене, перш за все, об'єктивною необхідністю у систематизації, структуризації, узагальненні, організації, управлінні, інтеграції тощо значних обсягів різноманітних знань та інформації, що накопичило людство на сьогоднішній день, а також історичним поширенням ідей системного підходу.

Методологічною основою системного підходу, зокрема в його сучасному розумінні та застосуванні, є **загальна теорія систем** *(general system theory)*, яка була започаткована Людвігом фон Берталанфі ще у 1930-х роках [1, 7]. Вона, декларує фундаментальні (системотворчі) чинники, що визначають і характеризують будь-яку систему: структура системи; елементний склад; взаємозв'язки між елементами; середовище, в якому система організована і функціонує.

У сучасній інтерпретації теорія систем визначається як загальнонаукова парадигма, яка пропонує холістичний підхід щодо дослідження систем. **Холістичний підхід** *(holistic approach)* – оцінка властивостей системи в цілому, з подальшим

вивченням (у разі необхідності) її складових [8]. Часто положення холістичного підходу пов'язують з поняттям *синергії* – це ефект, який полягає у тому, що при об'єднанні дії (взаємодії) двох або більше факторів результат буде більшим ніж сума результатів дії кожного з них окремо.

До застосування холістичного підходу вдаються вчені різноманітних галузей науки, зокрема біології, екології, філософії, психології, культурології, правознавства, політології й інших. В економічних науках, нині найвідомішим прикладом застосування холістичного підходу є «холістичний маркетинг» Ф. Котлера. У своїх останніх працях стосовно теорії маркетингу підприємств він схиляє фахівців до нового сприйняття ринкових і бізнес-процесів, зокрема в їхній єдності, взаємозв'язку, системності і частковості, при цьому беручи до уваги притаманну їм ентропію.

Аудит організацій у його сучасному розвитку і багатогранності, також потребує застосування ідей холізму і теорії систем. Наприклад, міжнародна робоча група з вивчення практики аудиту за стандартами ISO *(Auditing Practices Group – APG)*, яка діє в рамках міжнародної програми ISO/TC 176, і веде розробку керівних вказівок з аудиту системи менеджменту якості на відповідність вимогам цього стандарту, зазначає, що сучасні аудитори повинні керуватись системним підходом при підготовці та проведенні аудитів і бути готовими оцінювати одразу кілька сфер діяльності, за кількома напрямками, предметами й об'єктами аудиту. Відповідно, змінюються і вимоги до методології проведення аудитів. Вона повинна ґрунтуватись на результативності і постійному вдосконаленні, а висновки аудиторів додавати цінності підприємницькій діяльності в цілому.

Об'єктивна необхідність застосування холістичного підходу як фундаментальної основи теорії систем для цілісного дослідження складних об'єктів, явищ і процесів навколишнього світу, у тому числі економічних, у свою чергу, обумовлює доцільність і потребу керуватись цим підходом, при підготовці та проведенні аудиту середовища інформаційних технологій організацій.

Виходячи із зазначеної необхідності, а також сутності холістичного підходу, пропонується розробити **структурну модель** аудиту ІТ-середовища як цілісної системи – **холістичного ІТ-аудиту**, а також **організаційні моделі** аудиту кожної з її складових.

За основу структурної моделі холістичного ІТ-аудиту пропонується взяти структуру типового ІТ-середовища як цілісної системи, визначивши її елементний склад, взаємозв'язки між елементами, а також середовище, в якому вони функціонують і взаємодіють між собою.

Керуючись міжнародними стандартами, керівництвами і найкращим досвідом *(best practice)* в галузі управління ІТ [2-4], під структурою типового ІТ-середовища як системи пропонується розуміти цілісність трьох ключових підсистем: ІТ-інфраструктури *(IT infrastructure)*, ІТ-підрозділу *(IT department)* і ІТ-безпеки *(IT security)* (див. рис. 2.1). У науковому і практичному середовищі виділені підсистеми не мають однозначного трактування. Не вдаючись до аналізу різних думок [1-6], пропонуємо такі їх визначення: **ІТ-інфраструктура** – це ІТ-ресурси, що мають певний потенціал для задоволення цілей бізнесу; **ІТ-підрозділ** – це інтелектуальні (людські) ресурси, що перетворюють потенціал ІТ-ресурсів у реальні вигоди для бізнесу (досягнення бізнес-цілей, конкурентні переваги тощо); **ІТ-безпека** – це заходи і засоби, що забезпечують стан захищеності ІТ-середовища від загроз інформаційної безпеки, а також можливість ІТ-підрозділу реалізувати потенціал ІТ-ресурсів на достатньому для досягнення цілей бізнесу рівні.

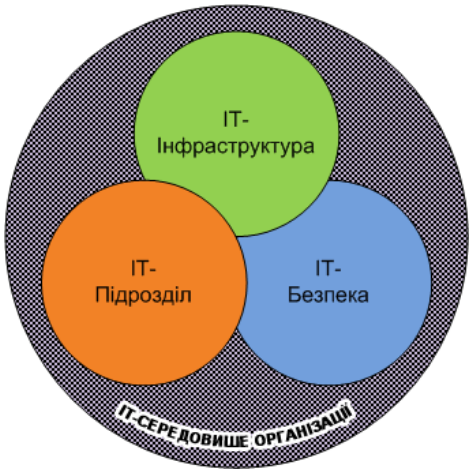


*Рис. 2.1 – Структура типового ІТ-середовища організації*

З метою визначення взаємозв'язків між структурними підсистемами типового ІТ-середовища, розглянемо їх більш детально.

**Інфраструктура інформаційних технологій організації** (інформаційна інфраструктура, ІТ-інфраструктура) – це комплекс взаємопов'язаних технологій, апаратних, програмних та обчислювальних засобів, систем зв'язку та телекомунікацій, впроваджених для розв'язання конкретних бізнес-задач і досягнення бізнес-цілей організації. Основні задачі цієї підсистеми ІТ-середовища полягають у задоволенні інформаційних, комунікаційних і обчислювальних потреб організації; автоматизації, комп'ютеризації та інформатизації бізнес-процесів; технологічній, інтелектуальній й аналітичній підтримці персоналу (людських ресурсів) і керівництва бізнес-підрозділів при виконанні функціональних обов'язків та прийнятті управлінських рішень; підвищенні продуктивності та ефективності господарської

діяльності за рахунок ІТ; створенні додаткових конкурентних переваг тощо. До функціональних елементів ІТ-інфраструктури організації пропонується відносити: апаратне забезпечення, програмне забезпечення, інформаційні системи, бази і сховища даних, комп'ютерні мережі, засоби комутованого і некомутованого телефонного, мобільного та радіозв'язку, web-ресурс тощо.

**Підрозділ управління інформаційними технологіями організації** (інформаційний підрозділ, ІТ-підрозділ) – це структурний підрозділ організації, головним завданням якого є забезпечення відповідності інформаційної інфраструктури цілям і потребам бізнесу. Керуючись передовим досвідом в галузі організації й управління ІТ [2, 4], можна виділити такі ключові напрямки діяльності ІТ-підрозділу і відповідні їм задачі: *планування та організація* (розробка стратегічних, тактичних й оперативних планів розвитку ІТ-інфраструктури організації, контроль за їх виконанням, аналіз показників, коригування за необхідності; планування ІТ-ресурсів: ІТ-бюджет, людські ресурси, обладнання і комплектуючі, зовнішні послуги тощо; розробка архітектури ІТ-інфраструктури й стандартів менеджменту ІТ-процесів відповідно до потреб бізнесу; визначення політик, правил, норм, стандартів, сценаріїв тощо стосовно інформаційної безпеки, контроль за їх впровадженням і дотриманням, коригування у разі потреби; планування ІТ-сервісів; управління якістю; оцінка й аналіз інформаційних ризиків; менеджмент ІТ-персоналу та ін.); *розробка/придбання і впровадження* (інформаційний маркетинг; придбання і супровід прикладних ІТ-рішень; управління проектами розробки і впровадження програмного забезпечення та інновацій; управління проектами реінжинірингу бізнес-процесів; управління змінами та ін.); *експлуатація і супровід* (надання ІТ-сервісів іншим структурним підрозділам згідно затверджених угод; облік ІТ-активів та операцій з ними; управління інформаційною безпекою та усунення наслідків і причин аварійних, помилкових і зловмисних ситуацій; управління мережевим «трафіком»; інвентаризація ІТ-активів; технічна підтримка і навчання користувачів ІТ; підготовка звітності; управління конфігураціями, проблемами, інцидентами, даними, операціями та ін.); *моніторинг і оцінка* (спостереження і оцінка ІТ-процесів; спостереження і оцінка внутрішнього контролю; гарантування відповідності ІТ-менеджменту вимогам регулюючих норм; забезпечення можливості проведення незалежного ІТ-аудиту та ін.). До функціональних елементів ІТ-підрозділу організації пропонується відносити: ІТ-директора (*Chief information officer - CIO*) та інше керівництво ІТ-підрозділу, фахівців з адміністрування й аналізу систем, фахівців з технічної підтримки, фахівців

з web-технологій, фахівців з інформаційного маркетингу, фахівців з проектування, розробки і впровадження програмних рішень тощо.

**Безпека інформаційної інфраструктури організації** (інформаційна безпека, IT-безпека) – це комплекс впроваджених організаційних заходів, програмно-технічних і фізичних засобів захисту IT-ресурсів й організації в цілому від загроз інформаційної безпеки, які є причиною ризиків IT-середовища. Загрози IT-безпеки здатні не лише порушити конфіденційність *(confidentiality)*, цілісність *(integrity)*, доступність *(availability)* інформаційних ресурсів тощо, але й завдати збитків організації в цілому, порушивши неперервність бізнесу *(business continuity)*. Основними задачами цієї підсистеми є: впровадження, визначених на рівні вищого IT-керівництва, політик, правил, норм, стандартів, сценаріїв тощо стосовно інформаційної безпеки у процеси інформаційної інфраструктури організації; розгортання в масштабі IT-середовища системи контрзаходів, необхідних для протидії ризикам IT-середовища; попередження, виявлення і реагування на інциденти порушення інформаційної безпеки (усунення наслідків і причин виникнення), звітування керівництву IT-підрозділу про результати; встановлення відповідності стану інформаційної безпеки організації вимогам еталонів обраних для порівняння (стандарти, кращі практики, вимоги законодавства тощо); донесення вимог і заходів інформаційної безпеки до кожного співробітника організації тощо. До функціональних елементів IT-безпеки в організації пропонується відносити: керівника відділу інформаційної безпеки; фахівців з інформаційної безпеки; систему управління інформаційною безпекою (СУІБ); організаційні заходи, програмно-технічні і фізичні засоби інформаційної безпеки тощо.

Взаємозв’язки між підсистемами структури типового IT-середовища організації покажемо на рисунку (див. рис.2.2):

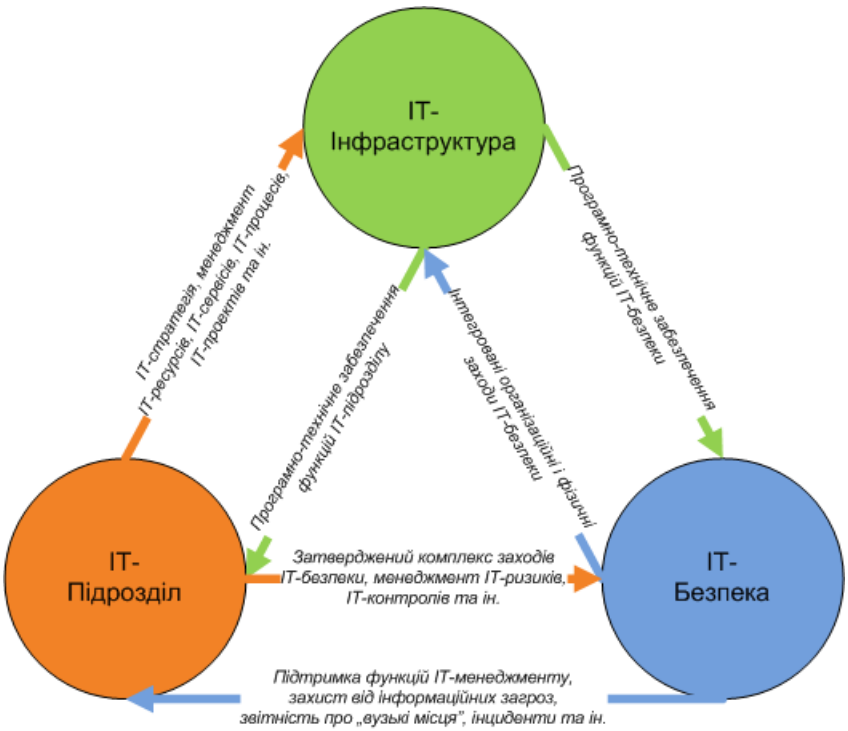


*Рис. 2.2 – Взаємозв'язки між підсистемами структури типового IT-середовища організації*

Під середовищем функціонування і взаємодії виділених підсистем, зокрема з точки зору IT-аудиту, пропонується розуміти **середовище IT-ризику**. Такий ризик пов'язаний із застосуванням інформаційних технологій в цілях бізнесу, і визначається, як імовірність виконання дії або настання події, яка реалізуючи загрозу інформаційної безпеки, може завдати шкоди організації, зокрема через вплив на її IT-середовище (вразливості IT-ресурсів) [1-3]. Високий рівень ризику IT-середовища впливає, перш за все, на здатність реалізувати потенціал IT-ресурсів організації для досягнення цілей бізнесу, а також на можливість досягнення цілей IT-аудиту.

Противагою середовищу IT-ризику є заходи ризик-менеджменту організації щодо IT, які також є невід'ємною складовою єдиного середовища функціонування і взаємодії виділених підсистем. Суть ризик-менеджменту IT-середовища організації полягає у виборі її керівництвом обґрунтованого набору контрзаходів для зниження рівня IT-ризику до прийнятного рівня. Такі контрзаходи є, по суті, елементами єдиної системи внутрішнього контролю (IT-контролями) ризиків IT-середовища. Доцільність застосування саме терміну «контроль» (від англ. *control*), на відміну від терміну «управління», для опису даної системи контрзаходів, зумовлена змістовим відтінком, який більш точно описує характер застосування таких заходів для зазначених цілей.

На підставі зазначеного вище опису типового IT-середовища організації як цілісної системи, структурну модель проведення IT-аудиту із застосуванням холістичного підходу (холістичного IT-аудиту) покажемо на рисунку (див. рис.2.3):

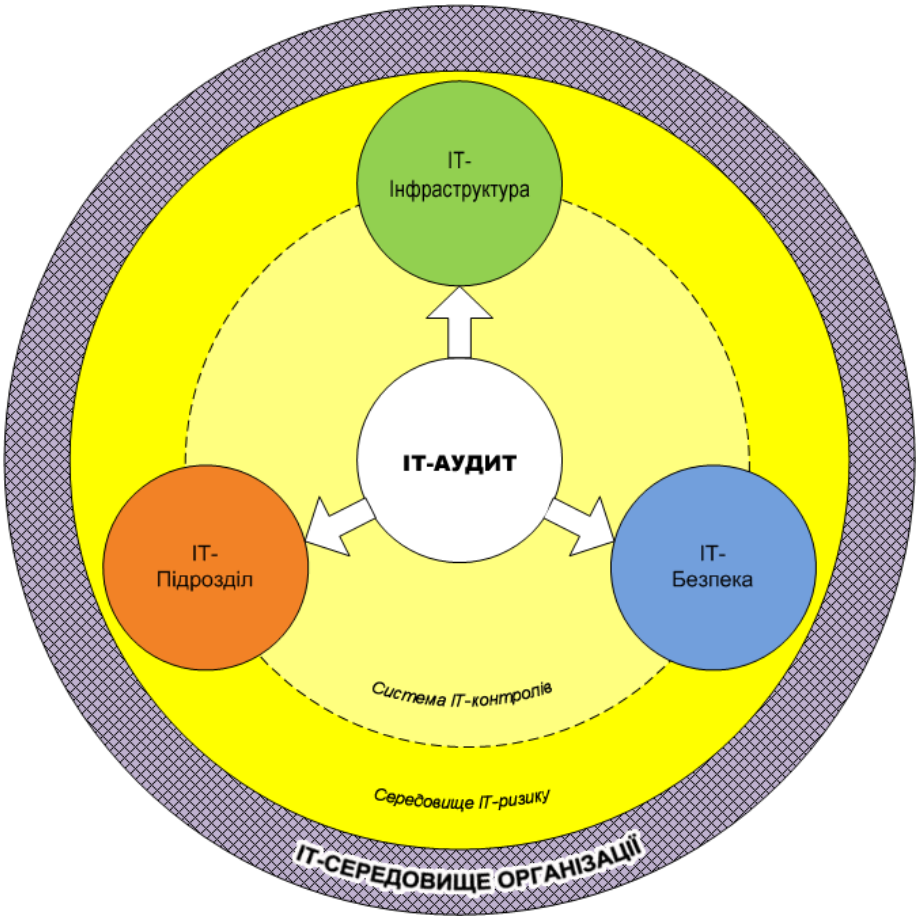


*Рис. 2.3 – Структурна модель холістичного IT-аудиту*

Холістичний підхід, застосований в моделі, декларує необхідність дослідження підсистем IT-середовища організації як взаємопов'язаних і взаємодіючих складових єдиної цілісної системи для досягнення максимального синергетичного ефекту від IT-аудиту. Запропонована модель є ризико-орієнтованою, тобто рівень ризику IT-середовища визначає пріоритет функціональних напрямків, об'єктів, заходів, методів IT-аудиту тощо, а також загальну доцільність його проведення, виходячи з можливості досягнення поставлених цілей. Холістичний IT-аудит згідно структурної моделі пропонується організувати як комплекс функціональних аудитів IT-інфраструктури, IT-підрозділу та IT-безпеки, в організаційних моделях яких пропонується визначити мету, цілі, ініціацію, об'єкти, заходи, методи і результати їх проведення (див. табл.2.1-2.3). Практичне застосування запропонованих моделей аудиту інформаційних технологій дозволить: *по-перше*, впровадити в організації системний підхід щодо управління IT-середовищем; *по-друге*, розробити технологію проведення холістичного аудиту інформаційних технологій; *по-третє*, ефективно підібрати і комбінувати методи функціональних видів IT-аудиту для цілісного і максимально ефективного дослідження IT-середовища, уникаючи фрагментарності, невизначеності, недостатньої щільності тощо.

*Таблиця 2.1 – Організаційна модель аудиту інфраструктури інформаційних технологій організації*

| **Аудит IT-інфраструктури** |
|---|
| ***Мета (goal):*** |
| надання обґрунтованого аудиторського висновку щодо поточного стану, сильних і слабких сторін інформаційної інфраструктури організації, а також рекомендацій щодо її удосконалення для задоволення потреб бізнесу. |
| ***Цілі (objectives):*** |
| *загальні:* **1)** оцінити і проаналізувати продуктивність, ефективність, економічність, достатність IT-інфраструктури тощо для задоволення потреб, вирішення задач і досягнення цілей бізнесу, а також виявити можливі шляхи покращення; **2)** встановити відповідність інформаційної інфраструктури затвердженій IT-стратегії, а також, за необхідності, певним еталонам (стандартам, кращим практикам, критеріям зрілості тощо); **3)** виявити "вузькі місця" (недоліки, невідповідності, інциденти тощо) в IT-інфраструктурі; **4)** отримати аудиторський висновок і рекомендацій за визначеними цілями аудиту та ін.<br>У кожному конкретному випадку аудиту зазначені вище цілі можуть бути конкретизовані і деталізовані відповідно до потреб його замовника, наприклад: **1)** оцінити достовірність даних в інформаційних системах організації; **2)** виявити і усунути причини надмірного навантаження на комп'ютерну мережу тощо. |
| ***Ініціація (initiation):*** |
| **1)** плановий аудит; **2)** позаплановий аудит; **3)** в рамках іншого аудиту (наприклад, фінансового, комплексного IT-аудиту тощо); **4)** сертифікація; **5)** зміна моделі бізнесу або окремих бізнес-процесів (реінжиніринг); **6)** проектування (розробка) або придбання складних програмно-технічних рішень; **7)** реструктуризація, злиття, ліквідація тощо. |
| ***Об'єкти (objects):*** |
| **1)** бізнес-процеси; **2)** IT-стратегія; **3)** апаратне забезпечення; **4)** програмне забезпечення; **5)** інформаційні системи; **6)** бази і сховища даних; **7)** комп'ютерні мережі; **8)** телефонія; **9)** web-ресурс тощо.<br>У кожному конкретному випадку аудиту зазначені вище об'єкти можуть бути конкретизовані і деталізовані відповідно до потреб його замовника, наприклад: **1)** окремий сегмент комп'ютерної мережі; **2)** конкретні сервери; **3)** робочі станції певного бізнес-підрозділу тощо. |
| ***Заходи (actions, measures, arrangements):*** |
| **1)** оцінка й аналіз рівня автоматизації і програмно-технічної підтримки бізнес-процесів; **2)** інвентаризація апаратного забезпечення; **3)** інвентаризація ліцензій програмного забезпечення; **4)** аналіз достовірності документів в інформаційних системах; **5)** аналіз випадків помилок, збоїв, злочинних дій та інших інцидентів в IT-інфраструктурі; **6)** оцінка та аналіз сукупної вартості володіння інформаційною інфраструктурою; **7)** перевірка заходів резервного копіювання даних; **8)** оцінка та аналіз повернення інвестицій в IT та ін. |
| ***Методи (approaches, methods):*** |
| **1)** *інспекційні* (фізична перевірка, анкетування, побудова структурних схем та ін.); **2)** *аналітичні* (оцінка IT-ризику, TCO, EVA, ROI та ін.); **3)** *еталонні* (ISO 900x, ISO 38500, ISO 15504, COBIT, ITIL, CMMI, SSADM та ін.). |
| ***Результати (results):*** |
| **1)** аудиторський висновок стосовно поточного стану IT-інфраструктури організації, відповідно до визначених цілей, задач і обмежень аудиту, забезпечений аудиторськими доказами і свідоцтвами; **2)** рекомендації аудитора стосовно заходів, які необхідно виконати для усунення виявлених в інформаційній інфраструктурі недоліків, а також невідповідностей потребам бізнесу чи вимогам еталону, обраного для порівняння. |

*Таблиця 2.2 – Організаційна модель аудиту інформаційного підрозділу організації*

| **Аудит IT-підрозділу** |
|---|
| ***Мета (goal):*** |
| надання обґрунтованого аудиторського висновку щодо поточного стану, сильних і слабких сторін інформаційного підрозділу організації і його діяльності, а також рекомендацій щодо їх удосконалення для задоволення потреб бізнесу. |
| ***Цілі (objectives):*** |
| *загальні:* **1)** оцінити і проаналізувати ефективність, продуктивність, економічність, оперативність діяльності IT-підрозділу тощо для задоволення потреб, вирішення задач і досягнення цілей бізнесу, а також виявити можливі шляхи покращення; **2)** встановити відповідність діяльності інформаційного підрозділу затвердженій IT-стратегії і бізнес-стратегії, а також, за необхідності, певним еталонам (стандартам, кращим практикам, критеріям зрілості тощо); **3)** виявити "вузькі місця" (недоліки, невідповідності, інциденти тощо) в IT-підрозділі і його діяльності; **4)** отримати аудиторський висновок і рекомендацій за визначеними цілями аудиту та ін.<br>У кожному конкретному випадку аудиту зазначені вище цілі можуть бути конкретизовані і деталізовані відповідно до потреб його замовника, наприклад: **1)** перевірити фахову компетентність керівника IT-підрозділу; **2)** встановити чи перевищує рівень ризику IT-середовища організації допустиме значення; **3)** перевірити чи надаються IT-сервіси відповідно до затверджених угод з їх клієнтами тощо. |
| ***Ініціація (initiation):*** |
| **1)** плановий аудит; **2)** позаплановий аудит; **3)** в рамках іншого аудиту (наприклад, фінансового, комплексного IT-аудиту тощо); **4)** сертифікація; **5)** зміна моделі бізнесу або окремих бізнес-процесів (реінжиніринг); **6)** реструктуризація, злиття, ліквідація; **7)** зміна IT-стратегії або тактики; **8)** зміна стандартів, норм і правил IT-менеджменту; **9)** низький рівень зрілості IT-процесів; **10)** високий рівень незадоволення клієнтів IT-сервісів тощо. |
| ***Об'єкти (objects):*** |
| **1)** бізнес-стратегія; **2)** бізнес-процеси; **3)** IT-стратегія, тактика і поточні плани; **4)** IT-процеси; **5)** затверджені стандарти, норми і правила IT-менеджменту; **6)** IT-бюджет/IT-витрати; **7)** IT-проекти; **8)** організаційна структура і функціональні обов'язки персоналу IT-підрозділу; **9)** IT-сервіси; **10)** угоди з клієнтами IT-сервісів; **11)** запити користувачів IT-інфраструктури та IT-сервісів у тому числі; **12)** IT-ризики/IT-контролі та ін.<br>У кожному конкретному випадку аудиту зазначені вище об'єкти можуть бути конкретизовані і деталізовані відповідно до потреб його замовника, наприклад: **1)** план відновлення працездатності інформаційних систем у випадку їх пошкодження або знищення; **2)** політики і процедури резервного копіювання даних тощо. |
| ***Заходи (actions, measures, arrangements):*** |
| **1)** оцінка рівня зрілості IT-процесів; **2)** оцінка та аналіз сукупної вартості володіння IT-підрозділом; **3)** аналіз IT-витрат за методикою П. Страсмана; **4)** аналіз збалансованих показників ефективності; **5)** оцінка економічного ефекту від роботи IT-підрозділу та ін. |
| ***Методи (approaches, methods):*** |
| **1)** *інспекційні* (інтерв'ю, анкетування, CAATs та ін.); **2)** *аналітичні* (оцінка IT-ризику, TCO, BSC та ін.); **3)** *еталонні* (ISO 20000x, COBIT, ITIL, ITSM, MOF, MSF, IRM та ін.). |
| ***Результати (results):*** |
| **1)** аудиторський висновок стосовно поточного стану IT-підрозділу організації, відповідно до визначених цілей, задач і обмежень аудиту, забезпечений аудиторськими доказами і свідоцтвами; **2)** рекомендації аудитора стосовно заходів, які необхідно виконати для усунення виявлених в інформаційному підрозділі і його діяльності недоліків, а також невідповідностей потребам бізнесу чи вимогам еталону, обраного для порівняння. |

*Таблиця 2.3 – Організаційна модель аудиту інформаційної безпеки організації*

| **Аудит IT-безпеки** |
|---|
| ***Мета (goal):*** |
| надання обґрунтованого аудиторського висновку щодо поточного стану, сильних і слабких сторін інформаційної безпеки організації, а також рекомендацій щодо її удосконалення для задоволення потреб бізнесу. |
| ***Цілі (objectives):*** |
| *загальні:* **1)** оцінити і проаналізувати ефективність, економічність, надійність IT-безпеки тощо для задоволення потреб, вирішення задач і досягнення цілей бізнесу, а також виявити можливі шляхи покращення; **2)** встановити відповідність інформаційної безпеки затвердженим політикам, сценаріям, нормам, правилам та IT-стратегії, а також, за необхідності, певним еталонам (стандартам, кращим практикам, критеріям зрілості тощо); **3)** виявити "вузькі місця" (недоліки, невідповідності, інциденти тощо) в IT-безпеці; **4)** отримати аудиторський висновок і рекомендацій за визначеними цілями аудиту та ін.<br>У кожному конкретному випадку аудиту зазначені вище цілі можуть бути конкретизовані і деталізовані відповідно до потреб його замовника, наприклад: **1)** виявити і усунути причини певного виду інцидентів інформаційної безпеки; **2)** оцінити ефективність впроваджених заходів ризик-менеджменту IT-середовища тощо. |
| ***Ініціація (initiation):*** |
| **1)** плановий аудит; **2)** позаплановий аудит; **3)** в рамках іншого аудиту (наприклад, фінансового, комплексного IT-аудиту тощо); **4)** сертифікація; **5)** зміна моделі бізнесу або окремих бізнес-процесів (реінжиніринг); **6)** реструктуризація, злиття, ліквідація; **7)** зміна затверджених політик, сценаріїв, стандартів, норм, правил інформаційної безпеки тощо; **8)** високий рівень ризику IT-середовища; **9)** розслідування інцидентів, пов'язаних з порушенням інформаційної безпеки; **10)** впровадження нових програмно-технічних засобів IT-безпеки тощо. |
| ***Об'єкти (objects):*** |
| **1)** бізнес-процеси; **2)** IT-стратегія; **3)** політики, сценарії, стандарти, норми, правила тощо інформаційної безпеки; **4)** організаційна структура і функціональні обов'язки персоналу з IT-безпеки; **5)** система управління інформаційною безпекою; **6)** програмно-технічні засоби інформаційної безпеки; **7)** середовище IT-ризику/система IT-контролів та ін.<br>У кожному конкретному випадку аудиту зазначені вище об'єкти можуть бути конкретизовані і деталізовані відповідно до потреб його замовника, наприклад: **1)** антивірусні та антиспамові заходи інформаційної безпеки; **2)** засоби шифрування конфіденційних даних; **3)** політика паролів і авторизації тощо. |
| ***Заходи (actions, measures, arrangements):*** |
| **1)** оцінка й аналіз середовища IT-ризиків і відповідних контрзаходів; **2)** оцінка й аналіз сукупної вартості володіння IT-безпекою; **3)** оцінка й аналіз ефективності, надійності і достатності організаційних заходів, програмно-технічних та фізичних засобів інформаційної безпеки; **4)** оцінка й аналіз рівня конфіденційності, цілісності і доступності інформаційних ресурсів; **5)** аналіз інцидентів IT-безпеки та ін. |
| ***Методи (approaches, methods):*** |
| **1)** *інспекційні* (інтерв'ю, анкетування, аудиторська вибірка та ін.); **2)** *аналітичні* (оцінка IT-ризику, TCO, ROSI та ін.); **3)** *еталонні* (ISO 2700x, ISO 15408, COBIT, ITIL, BSI\IT, SCORE, FIPS 197, FIPS 112 та ін.). |
| ***Результати (results):*** |
| **1)** аудиторський висновок стосовно поточного стану IT-безпеки організації, відповідно до визначених цілей, задач і обмежень аудиту, забезпечений аудиторськими доказами і свідоцтвами; **2)** рекомендації аудитора стосовно заходів, які необхідно виконати для усунення виявлених в інформаційній безпеці недоліків, а також невідповідностей потребам бізнесу чи вимогам еталону, обраного для порівняння. |

**Висновки**

Сучасне різноманіття напрямків і методів IT-аудиту з одного боку дає змогу запропонувати замовнику спеціалізований консалтинг, а з іншого є джерелом невизначеності стосовно ефективної технології його проведення і, відповідно, кінцевого результату. Часткове дослідження IT-середовища може виявитись менш витратним при одноразовому застосуванні, однак не зможе забезпечити замовнику належний рівень оцінки й аналізу (не дасть змоги побачити повну «картину», реальний стан справ і причинно-наслідкові залежності), тим паче, що ефективне застосування аудиту в управлінні організацією передбачає регулярність його проведення.

Запропоновані нами моделі холістичного IT-аудиту дозволяють цілісно дослідити IT-середовище, виходячи з його усвідомлення як єдиної системи взаємопов'язаних і взаємодіючих елементів. Такий аудит може виявитись більш витратним ніж частковий, однак значно ефективнішим, зокрема при регулярному проведенні.

**Література**


1. An introduction to the Business Model for Information Security // ISACA, 2009. - 28 p.
2. COBIT 4.1 // IT Governance Institute, 2007. - 196 p.
3. Information technology - Security techniques - Information security risk management – BS ISO/IEC 27005:2008 // BSI, 2008. - 64 p.
4. ITIL v.3 – Lifecycle Publication Suite // OGC, 2007. – 1200 p.
5. Ус Р.Л. Вплив світової фінансової кризи на розвиток IT-індустрії // Бюлетень міжнародного нобелівського форуму, № 1 (3), - том 2: збірник наукових праць/ Гол. ред. Б.І. Холод. – Дніпропетровськ: ДУЕП, 2010. – С. 326-331.
6. Ус Р.Л. Інструментальні засоби підтримки процесу аудиту інформаційних технологій // Формування ринкової економіки: збірник наукових праць, вип. 24 / Відп. ред. О.О. Бєляєв. – К.: КНЕУ, 2010. - С. 571-584.
7. Общая теория систем. [Електронний ресурс] – Режим доступу: http://ru.wikipedia.org/wiki/Теория_систем.
8. Подход холистический. [Електронний ресурс] – Режим доступу: http://dic.academic.ru/dic.nsf/ecolog/817/ПОДХОД.