УДК 657.6

СКІЦЬКО Олексій Іванович
ВАВІЛЕНКОВА Анастасія Ігорівна

ПЛАНУВАННЯ ІТ-АУДИТУ

Постановка проблеми. На сучасному етапі важливим є питання розроблення методик вирішення проблеми впровадження комп'ютерних інформаційних технологій в аудиторську практику, що дасть змогу підвищити ефективність роботи аудиторів та покращить якість аудиторських перевірок.

У проєктуванні комп'ютерних інформаційних технологій аудиторської діяльності виділяють два принципових підходи до їх створення, а саме: застосування набору тестів, орієнтованих на введення сталої інформації та орієнтування на введення первинної інформації системи, що досліджується.

Комп'ютеризація аудиту передбачає використання мережевої архітектури та збереження даних у єдиній базі, до якої користувачі повинні мати розмежований доступ. Під час аудиту необхідно вирішити низку завдань: 1) установити організаційну форму обробки даних і рівень автоматизації прийняття рішень; 2) визначити правильність вибору завдань автоматизованої системи; 3) вивчити й оцінити систему обігу інформації в автоматизованій системі; 4) дати характеристику способам введення даних і формуванню записів системи; 5) перевірити правильність алгоритмів поводження інформаційної системи. Також вирішення потребує питання визначення напрямів проведення перевірок аудиторськими підрозділами та створення плану ІТ-аудиту для організації.

Аналіз останніх досліджень і публікацій. Дослідженню поняття ІТ-аудиту, загроз для систем і мереж, підключених до інтернету, ризиків, що виникають, присвятили свої праці такі вчені, як В. Гужва [1], І. Данилюк [2], М. Денисенко [3], С. Івахненков [4], K. Rehage [5], S. Hunt [5] та ін.

Однак на сьогодні проблематика методології проведення аудиту інформаційної системи, визначення алгоритму дій аудиторів на основних етапах проведення ІТ-аудиту розглянута недостатньо. ІТ-середовище являє собою складну систему, яка об'єднує програмні, технічні, людські, інформаційні й інші ресурси. Зазначене зумовлює потреби в підвищенні економічності й ефективності використання ІТ, усунення недоліків застосування, обґрунтування витрат. Усе більшого значення набуває застосування в системі управління організацій ІТ-аудиту. Потребують дослідження та визначення об'єкт і межі ІТ-аудиту, що впливає на планування та процедуру збирання доказів для підготовки висновку.

Метою статті є дослідження методології проведення аудиту інформаційної системи, виокремлення й опис

дій аудиторів під час основних етапів складання плану проведення ІТ-аудиту, визначення впливу планування й інших факторів оцінювання ризиків та якості інформаційних технологій.

Виклад основного матеріалу. При розробці плану аудиту враховується багато організаційних факторів, таких як: галузь організації, розмір доходу, тип, складність бізнес-процесів і географічне розташування. Два фактори, які безпосередньо впливають на оцінку ризику й визначення того, що підлягає аудиту в ІТ-середовищі, – це його компоненти та роль. У зв'язку з цим виникають запитання:

• Які технології використовуються для виконання щоденних функцій?

• ІТ-середовище відносно просте чи складне?

• ІТ-середовище централізоване чи децентралізоване?

• Як налаштовані бізнес-додатки?

• Частину чи всю діяльність з обслуговування ІТ передано аутсорсингу?

• Наскільки ІТ-середовище змінюється щороку?

Указані ІТ-фактори є одними з компонентів, які аудитори повинні розуміти, щоб адекватно оцінити ризики щодо організації та створення річного плану аудиту [1].

На додаток до факторів, що впливають на оцінювання ризику, важливо, щоб аудитори використовували підхід, який визначає вплив та ймовірність виникнення ризику; визначали високу, середню та зони з низьким рівнем ризику шляхом кількісного та якісного аналізу.

Компанії, що займаються інформаційними технологіями, перебувають у постійному стані інновацій і змін. Зміни в ІТ можуть перешкодити зусиллям ІТ-аудитора визначити та зрозуміти вплив ризиків. Щоб допомогти ІТ-аудиторам, компанія може [2]:

– щороку проводити незалежне оцінювання ІТ-ризиків, визначати нові технології, які впливають на організацію;

– ознайомлюватися із щорічним звітом ІТ-відділу, короткостроковими планами й аналізом впливу планових ініціатив на оцінку ІТ-ризиків;

– починати кожен ІТ-аудит із перегляду компонентів оцінювання ризиків;

– бути гнучкою у сфері ІТ-аудиту – відстежувати профіль ризиків організації, пов'язаних з ІТ, і запроваджувати процедури аудиту в міру його розвитку.

Існує декілька структур управління ІТ, які можуть допомогти внутрішньому аудиту розробити найвідповідніший підхід до оцінювання ризиків для організації. Це дасть змогу аудиторам визначити, де в середовищі знаходяться ризики, і надати вказівки щодо того, як керувати ризиками [3]. Деякі з найпоширеніших структур управління ІТ включають COBIT (англ. Control Objectives for Information and Related Technology («Контрольні цілі для інформаційних та суміжних технологій»)) – відкритий ІТ-стандарт, який містить низку документів зі стандартами щодо оптимізації управління ІТ: аудитом ІТ та ІТ-безпекою, створено Асоціацією з аудиту та контролю інформаційних систем (ISACA) спільно з Інститутом управління ІТ (ITGI), також the UK's Office of Government Commerce IT Infrastructure Library (ITIL) і серію стандартів 27000 Між-

народної організації зі стандартизації (ISO) [4].

Відображення бізнес-процесів, інвентаризація та розуміння ІТ-середовища, а також проведення оцінювання ризиків у масштабах компанії внутрішнім аудитором визначить, що потрібно перевіряти та як часто. GTAG (Global Technology Audit Guide) надає інформацію, яка використовується групами внутрішнього аудиту для визначення сфери аудиту в ІТ-середовищі, що є частиною ІТ-аудиту [5].

Через високий ступінь залежності організації від ІТ важливо, щоб внутрішні аудитори розуміли, як створити план аудиту ІТ, частоту аудитів, а також специфіку кожного аудиту. Із цією метою GTAG допомогає внутрішнім аудиторам:

– зрозуміти організацію та рівень отриманої ІТ-підтримки;

– визначити та зрозуміти ІТ-середовище;

– визначити роль оцінювання ризиків у визначенні сфери ІТ-аудиту;

– формалізувати річний план ІТ-аудиту.

GTAG надає приклад гіпотетичної організації, щоб показати внутрішнім аудиторам, як виконати кроки, необхідні для визначення середовища ІТ-аудиту.

Одним із головних обов'язків і складних завдань для аудиторів є створення плану аудиту організації. Як пояснюється в Стандарті Інституту внутрішніх аудиторів (ІІА):

• Планування – керівники аудиторних груп щонайменше раз на рік створюють плани, засновані на оцінюванні ризиків, для визначення пріоритетів діяльності внутрішнього аудиту, які мають узгоджуватися з планами організації.

• Керівники повинні розглядати консультаційні зобов'язання, виходячи з їхнього потенціалу додати цінність і покращити діяльність організації та діяльність з управління ризиками [5].

Щоб розробити план аудиту на основі оцінювання ризиків, керівники груп аудиту спочатку проводять оцінювання ризиків у масштабах компанії. Належне виконання відповідного оцінювання ІТ-ризику є частиною загального оцінювання ризику і життєво важливим компонентом практики управління ризиками в масштабах компанії, також критичним елементом для розроблення ефективного плану аудиту. Для багатьох організацій інформація та технології, які її підтримують, є найціннішими активами організації. Крім того, у сучасному конкурентному та швидко мінливому інформаційному середовищі керівництво має підвищені очікування щодо функцій ІТ: управління потребує підвищення якості, функціональності та простоти використання; скорочення часу доставки; постійно покращувати рівень обслуговування, вимагаючи, щоб це було досягнуто з меншими витратами.

Незалежно від методології або частоти заходів із планування аудиту група внутрішнього аудиту повинна спочатку отримати розуміння ІТ-середовища організації, перш ніж проводити аудит. Використання технологій є невід'ємною частиною діяльності організації. Від збирання, обробки та звітності бухгалтерської інформації до виробництва, продажу та розповсюдження продукції практично кож-

на бізнес-діяльність певною мірою залежить від використання технологій. Використання технологій розвинулося до того, що вони не лише підтримують бізнес-процес, але й у багатьох випадках є невід'ємною частиною контролю процесу. У результаті внутрішній контроль процесів і діяльності стає більш технологічним, а недоліки та відсутність цілісності в допоміжних технологіях значно впливають на операції та бізнес-цілі організації.

Однак розроблення ефективного плану ІТ-аудиту на основі оцінювання ризиків є складним завданням для внутрішніх аудиторів, особливо, якщо аудитори не мають достатнього досвіду в ІТ.

Результати кількох оглядів зовнішнього оцінювання якості показують, що розроблення відповідного плану ІТ-аудиту є однією з найслабших ланок діяльності внутрішнього аудиту. Часто замість проведення аудиту на основі оцінювання ризиків внутрішні аудитори перевіряють те, що вони знають, або доручають це іншим компаніям, дозволяючи їм вирішувати, що перевіряти.

Розглянемо методи вирішення цієї проблеми – як визначити, що має бути включено в сферу ІТ-аудиту, і як ці напрями аудиту можна організувати в аудиторських підрозділах, щоб створити ефективний план ІТ-аудиту для організації.

Визначення річного плану аудиту повинно відбуватися в межах систематичного процесу, щоб гарантувати розуміння та врахування всіх фундаментальних аспектів бізнесу та діяльності з підтримки ІТ-послуг. Тому важливо, щоб основа плану ґрунтувалася на цілях, стратегії та бізнес-моделі організації.

Першим кроком у визначенні річного плану ІТ-аудиту є розуміння бізнесу. Аудитори визначають стратегії, цілі компанії та бізнес-моделі, які дадуть їм змогу зрозуміти унікальні бізнес-ризики організації. Аудиторська група також має розуміти, як існуючі бізнес-операції та функції ІТ-обслуговування підтримують організацію.

Далі аудитори визначають ІТ-середовище. Це робиться за допомогою первинного підходу, що з'ясовує ключові бізнес-цілі та процеси, важливі програми, які підтримують бізнес-процеси, інфраструктуру, необхідну для бізнес-додатків, модель підтримки послуг організації для ІТ і роль загальної підтримки таких технологій як мережеві пристрої. Використовуючи ці технічні компоненти разом із розумінням процесів підтримки обслуговування та проєктів упровадження системи, аудитори зможуть провести повну інвентаризацію ІТ-середовища. Цей перелік становить основу для оцінювання вразливостей, що можуть вплинути на внутрішній контроль.

Після того, як аудитори отримають чітке уявлення про ІТ-середовище організації, третім кроком є виконання оцінювання ризиків – методології для визначення ймовірності події, що може перешкодити організації досягти своїх цілей і виконанню завдань ефективним і контрольованим способом.

Інформація й аналіз, отримані завдяки розумінню організації, інвентаризації ІТ-середовища та оцінюванню ризиків, передаються на останній етап, формалізуючи план аудиту. Ме-

тою плану аудиту є визначення того, на чому зосередити роботу аудитора з надання впевненості та консультації, щоб керівництво отримало об'єктивну інформацію для управління ризиками організації та контрольним середовищем.

Для визначення ефективного плану ІТ-аудиту найважливішим є початок роботи. Варто пам'ятати про те, що технологія існує лише для підтримки й досягнення цілей організації та становить ризик для організації, якщо її невдача призводить до неможливості досягти мети. Отже, спочатку визначаються цілі організації, стратегії, бізнес-модель і роль, яку технології відіграють у підтримці бізнесу. Це робиться, визначивши ризики, виявлені у використовуваних технологіях, і те, як кожен ризик може завадити організації досягти бізнес-мети. Результатом будуть правильні оцінки та дії керівництва.

Крім того, аудитори повинні ознайомитися з бізнес-моделлю організації. Оскільки кожна організація має чітку місію та набір бізнес-цілей і завдань, бізнес-моделі допомагають аудиторам ідентифікувати продукти чи послуги, які надає організація, а також її ринкову базу, канали постачання, процеси виробництва та створення продукції, механізми доставки. Фундаментальні знання цієї інформації допоможуть аудиторам зрозуміти унікальні бізнес-ризики й те, як технології підтримують існуючі бізнес-моделі та пом'якшують загальний профіль ризиків організації.

Для розуміння операційного середовища та його унікальних ризиків слід ураховувати різні фактори та методи аналізу. Це пояснюється тим, що складність середовища контролю в організації напряму впливає на її загальний профіль ризику та систему внутрішнього контролю. Визначаються важливі фактори, які слід ураховувати:

1. *Ступінь системної та географічної централізації (тобто розподіл ресурсів).* Модель організації може визначати структуру ІТ-функції. Наприклад, компанії, що працюють із децентралізованими бізнес-підрозділами, які мають автономію для прийняття оперативних рішень, можуть мати децентралізовану ІТ-операцію, більшу різноманітність додатків і більшу різноманітність розгорнутих продуктів. З іншого боку, у більш централізованих компаніях аудитори можуть знайти корпоративні програми та підтримку централізованої ІТ-інфраструктури.

При створенні сфери ІТ-аудиту слід приділити увагу узгодженню окремих аудитів із функцією управління, яка відповідає за цю сферу. Централізована модель надання ІТ може передбачати менш індивідуальні аудити, зосереджені на основних технологіях і корпоративних програмах. І навпаки, децентралізована модель доставки може потребувати більше аудиторських завдань для досягнення належного узгодження з підзвітністю керівництва.

2. *Застосовані технології.* Різноманітність системної архітектури організації визначатиме обсяг технічних знань, необхідних для функції внутрішнього аудиту, і кількість областей, які необхідно переглянути. Різноманітність може бути на будь-якому рівні ІТ-стеку – ключових ком-

понентів технічної інфраструктури програми, включаючи її програмний код, базу даних, операційну систему та мережеву інфраструктуру.

Наприклад, прикладний програмний код включає в себе набори комп'ютерних програм, керуючі файли, таблиці й інтерфейси користувача, які забезпечують функціональність для конкретних операцій, таких як облік, нарахування заробітної плати та закупівлі. Інші додатки можуть керувати критично важливою інформацією, такою як інженерні та проєктні дані, юридична й особиста медична інформація. Організація також може мати програми, які керують виробничими процесами, які зазвичай називають системами керування процесами.

З іншого боку, системи баз даних дають змогу зберігати, модифікувати та витягувати дані (наприклад: Oracle, Microsoft SQL Server і DB2), тоді як операційні системи виконують основні завдання комп'ютера, такі як обробка введень оператора; управління внутрішньою пам'яттю комп'ютера; а також забезпечення функцій жорсткого диску, дисплея та периферійних пристроїв. Приклади операційних систем включають варіації Windows і UNIX, установлені на комп'ютерах і серверах. Портативні пристрої, такі як персональні цифрові помічники та мобільні телефони, також потребують операційних систем.

Нарешті, мережі з'єднують комп'ютери та дають змогу їм спілкуватися один з одним. Вони складаються з фізичних компонентів, таких як комутатори, маршрутизатори, брандмауери, проводка та програми, що контролюють маршрутизацію пакетів даних. Мережі також розгортаються за допомогою радіочастотної технології, яку зазвичай називають бездротовими мережами.

Усі чотири рівні стеку є важливими для забезпечення автоматизованих систем і створюють ризики щодо доступності, цілісності та конфіденційності. Ступінь ризику залежить від критичності діяльності, яку технологія підтримує та дозволяє, а також від конфігурації та розгортання технології. Отже, чим більше різноманітності в кожному з цих рівнів, тим вищий профіль ризику організації. Наприклад, ІТ-відділам простіше керувати однорідним середовищем серверів Windows, на яких працює база даних SQL Server, для єдиної програми планування ресурсів підприємства, ніж різними операційними системами та платформами баз даних, що лежать в основі різних програм. Незважаючи на ідеальний варіант, перший сценарій може бути непрактичним для великої організації з різноманітними операціями або децентралізованою моделлю. Під час створення плану аудиту критичні ІТ-елементи слід визначати й оцінювати як частину методів.

3. *Ступінь налаштування*. Дуже часто налаштовані впровадження ускладнюють управління ІТ-активами. Стандартне програмне забезпечення покладається насамперед на підтримку постачальників, які мають високий рівень знань і досвіду щодо своїх продуктів. Коли програмне забезпечення постачальника – будь то програми, операційні системи чи інше допоміжне програмне забезпечення – модифіковано відповідно до потреб або процесу організації, передбачаєть-

ся велика частка власності та в рівняння входить більше ризику. Загалом, якщо приймають рішення про налаштування стороннього програмного забезпечення, організації повинні проводити аналіз витрат і вигод. Крім того, перевірки індивідуальних реалізацій також потребують більших технічних знань із боку аудиторів.

4. *Ступінь формалізованої політики та стандартів компанії (тобто її управління).* Метою програми управління ІТ є надання можливості організації краще керувати повсякденною діяльністю та ризиками в ІТ за допомогою політик і стандартів. Наприклад, організації з формалізованими політиками й стандартами, які керують управлінським наглядом і допомагають створити середовище контролю ІТ, мають більше шансів запровадити ефективну програму управління ІТ. Ці програми є ефективними, коли політика та стандарти передаються, розуміються, контролюються, застосовуються й оновлюються керівництвом.

Політики – це загальні, довгострокові заяви про принципи, які стосуються операційних цілей керівництва; мають на меті довгостроковий ефект у керуванні розробкою бізнес-правил для конкретних ситуацій і можуть бути інтерпретовані й підтверджені стандартами, засобами контролю та настановами. Що стосується ІТ, політики можуть надавати керівні директиви високого рівня в таких сферах, як права інтелектуальної власності, захист даних, збереження та конфіденційність, щоб забезпечити відповідність законам і нормам та ефективний захист даних.

З іншого боку, стандарти описують обов'язковий процес або процедуру та надають подальші вказівки щодо того, як дотримуватися політики, з якою вони пов'язані. ІТ-стандарти зазвичай є технологічно нейтральними та можуть бути додатково визначені за допомогою специфічних для технології засобів контролю та вказівок (тобто параметрів або процедур конфігурації), які визначають, як слід упроваджувати стандарт.

Організації повинні запровадити постійний процес підтримки для всіх політик і стандартів, які стосуються останніх регуляторних мандатів. Наприклад, нещодавні зміни до Федеральних правил цивільного судочинства США, які регулюють надання доказів у судових справах, стосуються виявлення та отримання інформації, що зберігається в електронному вигляді. Через ці зміни рівень ризику організації частково залежить від дотримання нею оновлених політик і стандартів зберігання записів, які передбачають управління інформацією, що зберігається в електронному вигляді.

Доступні різні структури та методології управління ІТ, зокрема COBIT, стандарт ISO 27002 щодо управління інформаційною безпекою, Інструкції з контролю ІТ Канадського інституту дипломованих бухгалтерів і Стандарт належної практики інформаційної безпеки Форуму інформаційної безпеки. Ці структури забезпечують структурований спосіб категоризації цілей контролю та сфер контролю в усьому середовищі контролю. Організації можуть прийняти одну з цих структур

або використовувати їх як еталон при розробці власних.

5. *Ступінь регламентації та відповідності.* Організації в строго регульованих галузях матимуть переважно профіль високого ризику через потенційні наслідки недотримання нормативних вимог. Однак успішні організації в суворо регульованих галузях також мають визначене середовище контролю й ефективний управлінський нагляд для забезпечення постійного дотримання нормативних вимог, що призводить до нижчого профілю залишкового ризику. Отже, нормативні вимоги організації слід належним чином ураховувати в профілі ризику та системі аудиту ІТ.

6. *Ступінь і спосіб аутсорсингу.* ІТ-аутсорсинг усе більше поширюється в багатьох організаціях через високу вартість і досвід, необхідні для надання неосновних послуг. Що стосується аутсорсингу, аудиторам важливо враховувати різні ризики, пов'язані з угодою про аутсорсинг під час розробки проєкту ІТ-плану аудиту. Ключові фактори включають те, як керівництво бачить свою роль у нагляді та моніторингу, специфічні для країни ризики та завершеність планів забезпечення безперервності постачання організації.

7. *Ступінь оперативної стандартизації.* Операційні процеси та процедури включають увесь життєвий цикл розробки системи, а також конфігурацію, зміни, інциденти, операції та дії з управління безпекою. Подібно до ступеня централізації та різноманітності розгорнутих технологій, рівень операційної стандартизації може впливати на надійність і цілісність ІТ-інфраструктури. Отже, організації, які застосовують стандартизовані процеси для своїх функцій надання послуг, збільшують свою здатність працювати як високоефективні.

8. *Рівень опори на технології.* Деякі організації інтенсивно користуються технологіями або використовують певну технологію, щоб виділитися серед своїх колег і конкурентів. Хоча технологія може покращити загальний внутрішній контроль за допомогою автоматизованих засобів контролю додатків, управління та внутрішні операційні процеси стають важливішими, оскільки збільшується залежність від ІТ. Крім того, оскільки організації все більше залежать від доступності та цілісності ІТ, функціональних можливостей для здійснення операцій і досягнення своїх цілей, значущість ІТ-ризиків у загальному профілі ризиків організації зростає. Отже, характер і ступінь, у яких організація покладається на технологію, повинні бути очевидними в оцінюванні ризику, що використовується для розробки плану аудиту ІТ.

Висновки. Розглянуті фактори ІТ-середовища разом із підходом до аудиту, який використовується для розуміння операцій організації та ІТ-інфраструктури, надають аудиторам інформацію, необхідну для переходу до наступного кроку процесу планування аудиту – визначення меж ІТ-аудиту та виконання оцінювання ризиків.

Чітке планування проведення аудиту визначає аспекти оцінки організації, а саме: надійність, безпеку, результативність, ефективність.

Визначення критеріїв аудиту адаптується до кожного окремого виду та об'єкта IT-аудиту.

Керівництво ухвалює рішення щодо використання критеріїв аудиту, рівня залучення керівництва, стандартів, інструментарію IT-аудиту, етапів IT-аудиту, аналізу даних, формування доказової бази та звіту IT-аудиту.

Список використаних джерел

1. Гужва В. М. Інформаційні системи і технології на підприємствах : навчальний посібник. Київ : КНЕУ, 2001. 400 с. URL: http://www.dut.edu.ua/uploads/l_1366_68707543.pdf (дата звернення: 16.09.2022).

2. Данилюк І. IT-аудит: проблеми та перспективи. *Модернізація національної системи управління державним розвитком: виклики і перспективи.* 2016. Ч. 2. С. 75–77. URL: http://econf.at.ua/publ/konferenciia2016_12_8_9/sekcija_5_ekonomichni_nauki/it_audit_problemi_ta_perspektivi/61-1-0-1467 (дата звернення: 16.09.2022).

3. Денисенко М. П., Колос І. В. Інформаційне забезпечення ефективного управління підприємством. *Економіка та держава*. 2006. № 7. С. 19–24. URL: http://dspace.nuft.edu.ua/jspui/handle/123456789/22141 (дата звернення: 17.09.2022).

4. Івахненков С. В. Поняття комп'ютерного контролю та аудиту. *Менеджмент* : збірник наукових праць. 2009. Вип. 11. С. 24–38. URL: http://ekmair.ukma.edu.ua/bitstream/handle/123456789/644/Ivakhnenkov_Poniattia%20kompiutemoho.pdf (дата звернення: 17.09.2022).

5. Kirk Rehage, Steve Hunt. Developing the IT Audit Plan. *The Growing Risks in Auditing Technology*. 2018. P. 29. URL: www.theiia.org/technology (дата звернення: 18.09.2022).

Анотація. У статті розглянуто актуальні питання щодо організації напрямів проведення перевірок аудиторськими підрозділами та створення ефективного плану IT-аудиту для організації. Оскільки технології стають усе більше невід'ємною частиною діяльності будь-якої організації, головним завданням для внутрішніх аудиторів є якнайкраще проведення оцінювання ризиків в інформаційних технологіях (IT-ризиків) і засобів контролю в масштабах консультаційних послуг. Тому аудитори повинні розуміти IT-середовище організації; програми та комп'ютерні операції, які є частиною IT-інфраструктури.

Завершення перевірки компонентів IT-інфраструктури надасть аудиторам

Abstract. The article deals with contemporary issues with regard to carry out audit monitoring and to create an effective IT audit plan for the organization. Modern technologies are becoming an integral part of any organization's activities, therefore the main priority for internal audit is to perform IT risk assessment and management control in consulting. Therefore, IT environment programs and computer operations as a part of the IT infrastructure have to be appreciated by auditors.

Monitoring of IT infrastructure will afford auditors to expose infrastructure vulnerability. The basis for assessing infrastructure vulnerability that affects internal organization structure is formed by the monitoring system of IT hardware, software, net-

інформацію про вразливі місця інфраструктури. Повна перевірка IT-обладнання, програмного забезпечення, мережі та компонентів даних становить основу для оцінювання вразливостей в IT-інфраструктурах, які можуть вплинути на внутрішню структуру. Системи та мережі, підключені до інтернету, наражаються на загрози, які не існують для автономних систем і мереж. Після того, як буде досягнуте належне розуміння IT-середовища, головний аудитор і група внутрішнього аудиту можуть виконати оцінювання ризиків і розробити план проведення аудиту.

Ключові слова: аудит, аудит інформаційних технологій, IT-аудит, IT-інфраструктура, ризики, план проведення аудиту.

work and data components. Systems and networks connected to the Internet are exposed to threats that do not exist for self-contained systems and networks. When thorough understanding of the IT environment has been achieved, the executive auditor and the internal audit group can perform the risk assessment and develop the audit plan.

Key words: audit, IT audit, IT infrastructure, risk, audit plan evolving.

УДК 35.746.1

СОЛОДКА Олена Маркіянівна

ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ ВЗАЄМОДІЇ ДЕРЖАВ У ГЛОБАЛЬНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Постановка проблеми. Двома ключовими характеристиками сучасного історичного періоду є глобалізація та інформаційно-комунікаційні технології. Останні виступають у ролі головної рушійної сили глобалізованих суспільств, в основі яких лежать знання та інформація, що привело до формування нового типу суспільного устрою – інформаційного суспільства, яке існує і розвивається на двох рівнях – національному та міжнародному. У міру його розвитку створюються умови для економічного зростання окремих країн, інтенсивного включення держав і цілих регіонів у світові інтеграційні процеси, формування єдиного інформаційного простору. Відтак зростає значущість інформації і знань, унаслідок чого економічний розвиток більшою мірою, ніж раніше, залежить від ідей і знань, а держави, які стимулюють технологічні інновації, посилюють свій вплив на міжнародній арені; розмиваються кордони між міжнародною та внутрішньою