УДК 330.341.1:336.225.674(477)

ПРОБЛЕМНІ ПИТАННЯ ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНИХ СИСТЕМ У СУЧАСНИХ УМОВАХ

Москаленко Ф.І. *– ст. викладач, Херсонський ДАУ*

Постановка проблеми. Під терміном аудит Інформаційної Системи розуміється системний процес отримання та оцінки об'єктивних даних про поточний стан ІС, дії і події, що відбуваються в ній, та встановлює рівень їх відповідності певному критерію і надає результати замовнику.

У даний час актуальність аудиту різко зросла. Це пов'язано із збільшенням залежності організацій від інформації і ІС. Ринок насичений апаратно-програмним забезпеченням, багато організацій з ряду причин (найбільш нейтральна з яких - це моральне старіння устаткування і програмного забезпечення) бачать неадекватність раніше вкладених коштів в інформаційні системи і шукають шляхи вирішення цієї проблеми. Таких варіантів може бути два: з одного боку - це повна заміна ІС, що тягне за собою великі капіталовкладення, з іншого - модернізація ІС. Останній спосіб вирішення цієї проблеми - менш дорогий, але відкриває нові проблеми, наприклад, що залишити з наявних апаратно-програмних засобів, як забезпечити сумісність старих і нових елементів ІС. Більш суттєва причина проведення аудиту полягає в тому, що при модернізації та впровадженні нових технологій їх потенціал повністю не реалізується. Аудит ІС дозволяє домогтися максимальної віддачі від коштів, що інвестуються у створення і обслуговування ІС. Крім того, зросла вразливість ІС за рахунок підвищення складності елементів цієї ІС, збільшення рядків коду програмного забезпечення, нових технологій передачі та зберігання даних. Спектр загроз розширився. Це обумовлено такими причинами: передача інформації по мережах загального користування; "Інформаційна війна" конкуруючих організацій; висока плинність кадрів з низьким рівнем порядності.

Стан вивчення проблеми. За даними деяких західних аналітичних агентств, до 95% спроб несанкціонованого доступу до конфіденційної інформації відбувається з ініціативи колишніх співробітників організації Проведення аудиту дозволить оцінити поточну безпеку функціонування ІС, оцінити ризики, прогнозувати і управляти їх впливом на бізнес-процеси організації, коректно і обґрунтовано підійти до питання надання безпеки інформаційних активів організації, основні з яких: ідеї; знання; проекти; результати внутрішніх обстежень.

У даний час багато системних інтеграторів декларують постачання повного, закінченого рішення. На жаль, у кращому випадку, все зводиться до проектування і постачання устаткування і програмного забезпечення. Побудова інформаційної інфраструктури "залишається за кадром" та до рішення не додається. Обмовимося, що в даному випадку під інформаційною інфраструктурою розуміється налагоджена система, що виконує функції обслуговування, контролю, обліку, аналізу, документування всіх процесів, що відбуваються в інформаційній системі.

Завдання досліджень. Усе частіше і частіше до системних інтеграторів,

проектних організацій, постачальників устаткування виникають питання такого змісту: що далі стосовно наявності стратегічного плану розвитку організації, місця і ролі ІС в цьому плані, прогнозування проблемних ситуацій ? Чи відповідає наша ІС цілям і задачам бізнесу? Чи не перетворився бізнес в придаток інформаційної системи? Як оптимізувати інвестиції в ІС? Що відбувається усередині цього "чорного ящика" - ІС організації? Збої в роботі ІС – як виявити і локалізувати проблеми? Як вирішуються питання безпеки та контролю доступу? Підрядні організації провели поставку, монтаж, пуско-наладку. Як оцінити їхню роботу? Чи є недоліки, якщо є, то які? Коли необхідно провести модернізацію устаткування і ПЗ? Як обґрунтувати необхідність модернізації? Як встановити єдину систему управління і моніторингу ІС? Які вигоди вона надасть?

Результати досліджень. Керівник організації, начальник відділу організації інформаційних технологій і програмування (ОІТП) повинні мати можливість отримувати достовірну інформацію про поточний стан ІС в найкоротші терміни. Чи можливо це? Чому весь час провадиться закупівля додаткового обладнання? Співробітники відділу ОІТП постійно чогось навчаються, чи є в цьому необхідність? Які дії робити в разі виникнення позаштатної ситуації? Які виникають ризики при розміщенні конфіденційної інформації в ІС організації? Як мінімізувати ці ризики? Як знизити вартість володіння ІС? Як оптимально використовувати сформовану ІС при розвитку бізнесу? На ці та інші подібні питання не можна миттєво дати однозначну відповідь. Тільки розглядаючи всі проблеми в цілому, взаємозв'язки між ними, ураховуючи нюанси і недоліки можна отримати достовірну, обґрунтовану інформацію. Для цього в консалтингових компаніях у всьому світі існує певна специфічна послуга - аудит Інформаційної Системи. Великі та середні аудиторські компанії утворили асоціації - союзи професіоналів в області аудиту ІС, які займаються створенням та супроводженням стандартів аудиторської діяльності у сфері ІТ. Як правило, це закриті стандарти, "ноу-хау", які ретельно охороняються.

Інформаційне законодавство України у 2011 році було оновлено з прийняттям Закону України "Про доступ до публічної інформації" та нової редакції Закону України "Про інформацію", які були прийняті 13 січня 2011 року Верховною Радою України та набрали чинності 10 травня 2011 року. А також були прийняті Укази Президента від 5 травня 2011 року N 547 "Питання забезпечення органами виконавчої влади доступу до публічної інформації" та від 5 травня 2011 року N 548 "Про першочергові заходи щодо забезпечення доступу до публічної інформації в допоміжних органах, створених Президентом України".

Нова редакція Закону України "Про інформацію" як базового нормативно-правового акта в інформаційній сфері надає нове визначення інформації - як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Цим Законом передбачений поділ за змістом інформації на такі види: інформація про фізичну особу, інформація довідково-енциклопедичного характеру, інформація про стан довкілля (екологічна інформація), інформація про товар (роботу, послугу), науково-технічна інформація, податкова інформація, правова інформація, статистична інформація, соціологічна інформація та інші види інформації.

Однак, існує асоціація ISACA, що займається відкритою стандартизацією аудиту ІС. ISACA (Асоціація аудиту і контролю інформаційних систем) розроб-

ляє підходи до проведення аудиту ІС, як окремої самостійної послуги, впорядкує і стандартизує її. Асоціація ISACA заснована в 1969 році і в даний час об'єднує близько 20 тисяч членів із понад 100 країн, у тому числі і з України. Асоціація координує діяльність більш ніж 12 тис. аудиторів інформаційних систем.

Основна декларована мета асоціації - це дослідження, розробка, публікація і просування стандартизованого набору документів по управлінню інформаційною технологією для щоденного використання адміністраторами і аудиторами інформаційних систем. На допомогу професійним аудиторам, керівникам ОІТП, адміністраторам і зацікавленим користувачам асоціацією ISACA і залученими фахівцями з провідних світових консалтингових компаній був розроблений стандарт CoBiT. CoBiT - контроль об'єктів інформаційних технологій - відкритий стандарт, перше видання якого в 1996 році було продано в 98 країнах по всьому світу і полегшило роботу професійних аудиторів у сфері інформаційних технологій. Стандарт пов'язує інформаційні технології і дії аудиторів, об'єднує і узгоджує багато інших стандартів в єдиний ресурс, що дозволяє авторитетно, на сучасному рівні одержати уявлення і управляти цілями і задачами, які розв'язуються ІС. CoBiT враховує всі особливості інформаційних систем будь-якого масштабу і складності. Основне правило, покладене в основу CoBiT, таке: ресурси ІС повинні управлятися набором природно згрупованих процесів для забезпечення організації необхідною і надійною інформацією.

А тепер трохи роз'яснень з приводу того, які ресурси та критерії їх оцінки використовуються в стандарті CoBiT.

Трудові ресурси - під трудовими ресурсами розуміються не тільки співробітники організації, але також керівництво організації і контрактний персонал. Розглядаються навички штату, розуміння завдань і продуктивність роботи.

Додатки - прикладне програмне забезпечення, використовуване в роботі організації.

Технології - операційні системи, бази даних, системи управління і т.д.

Устаткування - усі апаратні засоби ІС організації, з урахуванням їх обслуговування.

Дані - у самому широкому сенсі - зовнішні і внутрішні, структуровані і неструктуровані, графічні, звукові, мультимедіа і т.д.

Усі ці ресурси оцінюються CoBiT на кожному з етапів побудови або аудиту ІС за такими критеріями. Ефективність - критерій, що визначає доречність і відповідність інформації завданням бізнесу. Технічний рівень - критерій відповідності стандартам та інструкціям. Безпека - захист інформації. Цілісність - точність і закінченість інформації. Придатність - доступність інформації необхідним бізнес-процесам у сьогоденні і майбутньому. А також захист необхідних супутніх ресурсів. Узгодженість - виконання законів, інструкцій і домовленостей, що впливають на бізнес-процес, тобто зовнішні вимоги до бізнесу. Надійність - відповідність інформації, що надається керівництву організації, здійснення відповідного управління фінансуванням і узгодженість посадових обов'язків.

Застосування стандарту CoBiT можливо як для проведення аудиту ІС організації, так і для початкового проектування ІС. Звичайний варіант прямої і зворотної задач. Якщо в першому випадку - це відповідність поточного стану ІС кращий практиці аналогічних організацій і підприємств, то в іншому - спочатку вірний проект і, як наслідок, по закінченні проектування - ІС, яка прагне до ідеа-

лу. Надалі ми будемо розглядати аудит ІС, маючи на увазі при цьому, що на будь-якому етапі можливе вирішення зворотної задачі - проектування ІС.

Розглянемо переваги CoBiT перед численними західними розробками. Перш за все, це його достатність поряд з можливістю відносно легкої адаптації до особливостей вітчизняних ІС. І, звичайно ж, те, що стандарт легко масштабується і нарощується. CoBiT дозволяє використовувати будь-які розробки виробників апаратно-програмного забезпечення та аналізувати отримані дані, не змінюючи загальні підходи і власну структуру.

На етапі підготовки і підписання початково-дозвільної документації визначаються межі проведення аудиту: Межі аудиту визначаються критичними точками ІС (елементами ІС), в яких найбільш часто виникають проблемні ситуації. На підставі результатів попереднього аудиту всієї ІС (у першому наближенні) проводиться поглиблений аудит виявлених проблем. У цей же час створюється команда проведення аудиту, визначаються відповідальні особи з боку Замовника. Створюється і узгоджується необхідна документація. Далі проводиться збір інформації про поточний стан ІС із застосуванням стандарту CoBiT, об'єкти контролю якого отримують інформацію про всі нюанси функціонування ІС як у двійковій формі (Так / Ні), так і формі розгорнутих звітів. Детальність інформації визначається на етапі розробки вихідної дозвільної документації. Існує певний оптимум між витратами (тимчасовими, вартісними і т.д.) на отримання інформації та її важливістю і актуальністю.

Проведення аналізу - найбільш відповідальна частина проведення аудиту ІС. Використання при аналізі недостовірних, застарілих даних неприпустимо, тому необхідне уточнення даних, поглиблений збір інформації. Вимоги до проведення аналізу визначаються на етапі збору інформації. Методики аналізу інформації існують у стандарті CoBiT, але якщо їх не вистачає, не забороняється використовувати дозволені ISACA розробки інших компаній.

Результати проведеного аналізу є базою для вироблення рекомендацій, які після попереднього погодження з Замовником повинні бути перевірені на здійсненність і актуальність з урахуванням ризиків впровадження. Контроль виконання рекомендацій - важливий етап, що вимагає безперервного відстеження представниками консалтингової компанії ходу виконання рекомендацій. На етапі розробки додаткової документації проводиться робота, спрямована на створення документів, відсутність або недоліки в яких можуть викликати збої у роботі ІС. Наприклад, окреме поглиблене розглядання питань забезпечення безпеки ІС. Постійне проведення аудиту гарантує стабільність функціонування ІС, тому створення план-графіка проведення подальших перевірок є одним із результатів професійного аудиту.

Результати аудиту ІС організації можна розділити на три основні групи:

1. Організаційні - планування, управління, документообіг функціонування ІС.

2. Технічні - збої, несправності, оптимізація роботи елементів ІС, безперервне обслуговування, створення інфраструктури і т.д.

3. Методологічні - підходи до вирішення проблемних ситуацій, управління та контролю, загальна впорядкованість і структуризація.

Проведений аудит дозволить обгрунтовано створити такі документи: Довгостроковий план розвитку ІС, Політика безпеки ІС організації, Методологія

роботи і доведення ІС організації, План відновлення ІС в надзвичайній ситуації, Вимоги до подання інформації.

Щоб інформація була корисною, вона повинна володіти певними характеристиками, серед яких:

1. Зрозумілість. Інформація повинна бути зрозумілою для користувача, який володіє певним рівнем знань.

2. Доречність. Інформація є доречною або має відношення до справи, якщо вона впливає на рішення користувачів і допомагає їм оцінювати минулі, справжні, майбутні події або підтверджувати і виправляти минулі оцінки. На доречність інформації впливає її зміст і суттєвість. Інформація є суттєвою, якщо її відсутність або неправильна оцінка можуть вплинути на рішення користувача. Ще одна характеристика доречності - це своєчасність інформації, яка означає, що вся значима інформація своєчасно, без затримки включена у звіт і такий звіт наданий вчасно.

3. Достовірність, надійність. Інформація є достовірною, якщо вона не містить суттєвих помилок або упереджених оцінок і правдиво відображає господарську діяльність. Щоб бути достовірною, інформація має відповідати наступним характеристикам:

- Нейтральність - інформація не повинна містити однобоких оцінок, тобто інформація не повинна надаватися вибірково, з метою досягнення певного результату.

- Обачність - готовність до обліку потенційних збитків, а не потенційних прибутків і як наслідок - створення резервів. Такий підхід доречний у стані невизначеності і не означає створення прихованих резервів або спотворення інформації.

- Достатність інформації - включає таку характеристику, як вимога повноти інформації як з точки зору її суттєвості, так і витрат на її підготовку.

Висновки та пропозиції. Потреба вітчизняного ринку в даній послузі дуже велика. При оцінці необхідності проведення аудиту ІС необхідно акцентувати увагу на таких моментах: складності розв'язуваних завдань - постійне збільшення, як кількісне, так і якісне, завдань, що вирішуються ІС; розгалуженості ІС - складність в обслуговуванні, територіальна розподіленість; перспективності бізнесу - нові напрямки, ринки, умови роботи; керівництво організацією - вміння і бажання керівників стратегічно мислити, бачити перспективи, що відкриваються стандартизованим підходом, засновані на передовому досвіді.

Хто зацікавлений у проведенні аудиту? Перш за все, це комерційні або бюджетні організації та підприємства для обґрунтування інвестицій в ІС, системні інтегратори, ІТ компанії для оцінки впливу ІС на основний бізнес-процес і розширення спектра пропонованих послуг. Для компаній, що проводять фінансовий аудит - аудит ІС, додаткова послуга, яка здатна підвищити рейтинг компанії на ринку. Генеральним підрядникам робіт буде цікава можливість оцінити роботу субпідрядників в сфері ІТ. А також проведення аудиту ІС за стандартом CoBiT буде цікаво будь-яким підприємствам і організаціям, що мають або планують створення ІС і які зацікавлені в отриманні відповідей на питання, наведені на початку цієї статті.

Перспективи подальших досліджень. У всьому світі консалтинг у сфері аудиту придбав воістину всеосяжний розмах - "жодної серйозної справи без

аудиту". Але, незважаючи на це, при вивченні звітів про проведення аудиту ІС, в плані технічної грамотності і змістовності рекомендацій з'ясувалося, що рівень пропонованих замовникам звітів досить низький. Це пояснюється однією важливою причиною: переважна більшість західних аудиторських компаній, що пропонують свої послуги, у тому числі в сфері ІТ, виросли з фінансового аудиту та запрошують технічних фахівців лише у міру потреби. Тут споконвічно і закладено перевага вітчизняних українських компаній - системних інтеграторів: наявність висококваліфікованих фахівців з величезним практичним досвідом у різних сферах телекомунікаційного ринку дозволяє їм проводити аудит ІС як окрему специфічну послугу, без істотних змін в організаційній структурі. У разі, якщо ці організації візьмуть на озброєння професійний стандарт з апробованої і налагодженої структурою, то професіоналізм подібних послуг різко зросте.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. 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», 2011.
2. Лазарєва С.Ф., Ус Р.Л. Сучасні методи аудиту інформаційних технологій // Держава та регіони: науково-виробничий журнал – Запоріжжя., 2011.
3. http://zakon4.rada.gov.ua/laws/show/2657
4. COBIT 4.1 // IT Governance Institute, 2007. – 196 p.
5. Information technology – Security techniques – Information security risk management – BS ISO/IEC 27005:2008 // BSI, 2008. – 64 p.
6. Tommie Singleton. The COSO Model: How IT Auditors can use it to evaluate the effectiveness of internal controls (Part 1, Part 2) // Information Systems Control Journal, ISACA, 2007–2008. – 5 p.
7. http://gc.ua/uk/it

УДК 339.13.012

СВІТОВІ ТЕНДЕНЦІЇ РОЗВИТКУ РИНКУ КРУП'ЯНИХ І ОЛІЙНИХ КУЛЬТУР У КОНТЕКСТІ ПРОДОВОЛЬЧОЇ БЕЗПЕКИ УКРАЇНИ

***Орленко О.В.** - к.е.н., доцент,*
***Шевцов Д.В.** - здобувач, Міжнародний університет бізнесу і права*

Постановка проблеми. В останні десятиліття, незважаючи на прорив у технологіях та підвищення продуктивності виробництва продовольства, факт залишається фактом: їжа – основне джерело всіх людських потреб – перебуває поза межами досяжності близько мільярда людей в усьому світі.

Оскільки центральна складова безпеки людини – це свобода від страху та нужди, продовольчу безпеку можна розглядати як підсистему всезагальної концепції безпеки людини, оскільки наявність їжі і доступ до неї являє собою питання життя та смерті для всіх людей [2]. Тому продовольчу безпеку слід розглядати як основну проблему для кожної людини. За твердженням Продовольчої