УДК 004.056.5(.476)(.063)

МІЖНАРОДНА РЕГЛАМЕНТАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ ТА СТАНДАРТИЗАЦІЇ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Казакова Н.Ф., Плешко Е.А., Айвазова К.Б.

INTERNATIONAL REGULATION OF REGULATORY OF DOCUMENTS AS WELL STANDARDIZATION IN AREA AUDIT OF INFORMATION SECURITY

Kazakova N., Pleshko E., Aivazova K.

У статті, опираючись на зарубіжні публікації, проведено огляд нормативних та законодавчих документів, які регулюють технології аудиту інформаційної безпеки організацій. Показано, що закони продовжують розроблятися та удосконалюватися. Визначено, що актуальним питанням є вимоги до практичних дії зі сторони організацій щодо контролю за дотриманням вимог до інформаційної безпеки. Відзначено, що актуальним питанням є порядок визначення, чи виконують організації всі необхідні заходи з інформаційної безпеки.

Ключові слова: *DPA, CMA, GLBA, HIPAA. SOX, COSO, COBIT, ITIL, BS 15000, ISO/IEC 20000, ISO/IEC 15408, Р ИСО/МЭК 15408, ISO/IEC 17799, ISO/IEC 27001, EA-7/3.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими та практичними завданнями. Як показано у [1], прямих законодавчих вимог в області інформаційної безпеки (ІБ) та аудиту ІБ існує досить мало. Однак у більшості країн діють галузеві регулятивні документи, які нормують впровадження заходів щодо забезпечення ІБ. Крім того, з зазначеного питання розроблені настанови для здійснення контролю ефективності вживаних заходів. Деякі з документів є нормативами прямої дії. Це, наприклад, відноситься до галузей з високим рівнем регуляторного втручання, зокрема в сфері надання фінансових послуг та банківських операції. Інші документи створюються та повсюдно впроваджуються, як результат вимог до забезпечення захисту персональних даних (ЗПд) клієнтів, співробітників та інших зацікавлених у діяльності організацій осіб. Тут на першому плані стоять сфера охорони здоров'я в США та Європейська директива про ЗПд.

Зростаюче застосування засобів автоматизації при обробці інформації, призвело до концентрації у певних місцях інформації, що є критичною для організацій та їх клієнтів, у 80-х роках минулого століття привернуло до даної ситуації увагу законодавців: у першу чергу – в країнах з високорозвиненою економікою. Т.ч., визначився новий актуальний напрямок науково-практичних досліджень – розробка міжнародних документів з регулювання правових аспектів та стандартизації в області ІБ, який продовжується по теперішній час.

Виходячи зі сказаного, ***постановкою проблеми у загальному вигляді*** є огляд та аналіз поточних міжнародних документів з регулювання правових аспектів та стандартизації в області ІБ, а саме – її аудиту.

Аналіз останніх досліджень та публікацій показує, що першою з країн, які розробили законодавчі акти в області ІБ, а саме – з конфіденційності персональних даних, була Великобританія. У 1984 році вона прийняла перший закон про ЗПд (*Data Protection Act* – DPA) [2], який визначив основні положення та необхідність в області забезпечення ІБ громадян. Прийняття закону стимулювало розробку норм по забезпеченню конфіденційності в багатьох країнах. Ця дія вплинула на всі наступні процедури впровадження та оцінювання організаціями заходів з контролю в області ІБ. Нещодавно прийнятими у США законодавчими актами, що посилюють вимоги відносно корпоративного керування (наприклад, закон Сарбейнса-Окслі) [3], організаціям прямо пропонується приділяти більше уваги питанням внутрішнього контролю у всіх сферах, включаючи інформаційні технології (ІТ) та ІБ. Законодавство розраховане на забезпечення дотримання заходів безпеки та контролю на всіх рівнях: від операційних систем і баз даних до бізнес-додатків. Закон Сарбейнса-Окслі передбачає наявність заходів контролю на рівні організації, включаючи оцінку та моніторинг ризиків, у тому числі внутрішній контроль та аудит системи контролю в області ІТ та ІБ. У результаті багато організацій почали використовувати усілякі підходи до управління правами користувачів, застосовуючи їх як відповідь на комплексні та тверді вимоги закону Сарбейнса-Окслі в області ІБ.

Виходячи зі сказаного, ***метою статті є відображення стану*** правових аспектів та міжнародної стандартизації у галузі аудиту ІБ з метою їх практичного використання у вітчизняних організаціях.

Виклад основного матеріалу. В ідеальному світі кожна організація та будь-який її співробітник повинні розуміти ризики, пов'язані з

інформацією, і вживати заходи для її захисту відповідно до тієї цінності, яку вона представляє. При цьому необхідно зважати на те, яким загрозам піддається та наскільки вразлива інформаційна система (ІС) організації.

Прийнято вважати, що у майбутньому ідеальному суспільстві не буде людей, які б прагнули здобути користь з інформації, отриманої без дозволу. На жаль, сьогоднішні реалії говорять про інше: люди не завжди замислюються над тим, якою інформацією вони володіють і що вони повинні зробити для її захисту. Крім того, є особи, які бажають заради власної вигоди або просто заради жарту, застосувати у таких цілях погано організовану систему безпеки, та отримати доступ до інформації, не маючи на то повноважень. Розуміючи цю проблему, законодавчі та інші регулятивні органи продовжують розробляти закони та норми з метою підвищення рівня ІБ та стимулювати організації до відповідних до дій.

Як вже зазначалося, більшість перших прийнятих законодавчих актів та регулятивних норм в області ІБ, відносилися до ЗПд, які зберігаються в організаціях. Так, метою закону DPA, було спонукати організації належним чином забезпечити захист персональних даних, що зберігалися в них. В 1998 році DPA був удосконалений відповідно до нових вимог Європейського Союзу до конфіденційності персональної інформації. Розділ DPA, присвячений ІБ, невеликий, однак багато інших його положень вказують на важливість питань безпеки. Одним з найважливіших результатів прийняття та впровадження DPA стало те, що організації почали замислюватися над тим, якою інформацією вони володіють, яка інформація їм необхідна і як визначити вимоги до інформації (на основі її класифікації) з погляду безпеки. Тим більше питань виникло, коли стало ясно, що у DPA не має вимог щодо проведення регулярної перевірки стану ІБ, однак у ньому є розділ, що надає повноважень урядовому органу з захисту інформації можливості оцінювати рівень відповідності безпеки обробки персональних даних вимогам цього закону. Саме у відповідь на зазначене питання, урядовий орган (у Великобританії на той час – *Інформаційна інспекція*) видав посібник з перевірки з детальним описом аудиторської програми, яка може бути використана організаціями для самооцінки відповідності або використана третіми особами для перевірки відповідності закону. На жаль, вітчизняних аналогів такого посібника немає.

Однією з перших закон відносно «неналежного» використання технологій (*The Computer Misuse Act* – CMA) [4] також ввела в дію Великобританія в 1990 році. Він розглядає три види карних злочинів:

– неправомірний доступ до комп'ютерів (включаючи незаконне копіювання програм);

– неправомірний доступ з метою здійснення або сприяння здійсненню подальших правопорушень (наприклад, таких, як крадіжка та шахрайство);

– неправомірна зміна програмного забезпечення (у т.ч. – навмисне та неправомірне знищення програмного забезпечення, баз даних або впровадження вірусів).

На перший погляд може здатися, що цей закон мало впливає на діяльність організацій, якщо не зважати на почуття задоволеності від усвідомлення того, що зловмисники будуть покарані. Однак на ділі CMA вніс багато важливих положень для бізнесу. Так, для успішного судового переслідування, відповідно до CMA, організації необхідно мати, наприклад, достатній доказ того, що доступ до ІС не був санкціонований. CMA став всесвітньо відомий тим, що зобов'язав будь-яку особу, яка може використовувати комп'ютерну техніку, усвідомлювати, що вона не завжди має уповноваження на доступ до ІС. Саме внаслідок впровадження CMA, організації стали практикувати використання повідомлення при вході в систему, наприклад, такі, які ставлять до відома користувача, що система призначена тільки для авторизованих користувачів, а не вітання типу «Welcome!». Крім того, CMA стимулював організації чітко визначитися в частині політики «прийнятного використання» ІС, тобто що можна, а що не можна робити в даній області.

У західних країнах, практично без винятків, є чимало прикладів, коли фізичні особи, не переслідувалися у судових органах відповідно до CMA через відсутність надійних доказів (наприклад, відповідних журналів реєстрації подій або аудиторських лог-файлів) щодо втручання в роботу ІС. Частота подібних випадків спонукала організації уважніше ставитися до питань ІБ. У цьому сенсі слід зазначити, що всі діючі керівництва, які організації Великобританії можуть та повинні використовувати у своїй практичній діяльності, вільно розміщені у всесвітні мережі – www.informationcommissioner.gov.uk. Їх аналіз показав, що люба британська організація може самостійно провести аудит ІБ та своїх ІТ в цілому ще до того, як будуть заповнені відповідні журнали реєстрації та записані лог-файли.

Найбільш суперечливим положенням у CMA є поняття *легітимності несанкціонованого доступу* до інформаційної (комп'ютерної) системи (мережі). Під чинність CMA потенційно попадають процеси сканування на уразливість системи захисту та тести на проникнення (порушення периметру), які можуть бути проведені як сторонніми консультантами, так і власним персоналом організації з метою вдосконалювання системи ІБ. На сьогоднішній день британськими практиками з ІБ

обговорюються запропоновані фахівцями виправлення до CMA, які дозволять розширити сферу його застосування та включити в нього питання поширення і використання інструментарію для тестування систем ІБ для легітимних консультантів по безпеці.

США традиційно ніколи не були світовим лідером в області законодавства, що стосується забезпечення конфіденційності персональних даних та ІБ. Однак останнім часом у США був прийнятий цілий ряд регламентуючих документів та законів з зазначених питань. Істотний вплив на організації в США щодо ІБ та конфіденційності, виявив закон Гремма-Ліча Блілі (*Gramm-Leach Bliley Act* – GLBA) [5]. GLBA набув чинності у 1999 році. Його дія була спрямована на компанії, що надають фінансові послуги. Можливі санкції за невиконання вимог закону передбачувалися до тих компаній, які були не настільки ретельні у сенсі ІБ, як варто було б. Особливо це стосувалося забезпечення конфіденційності даних клієнтів банків. Аналогічно вимогам, які були розроблені у Європі майже десятиліття до введення GLBA, він першим почав вимагати від фінансових установ та афілійованих з ними організацій забезпечення ІБ, включаючи цілісність та конфіденційність персональних даних фізичних осіб. Так, відповідно до GLBA (який, наразі, діє у США до сьогоднішнього дня), фінансові установи повинні мати програму забезпечення ІБ, засновану на оцінці ризиків, що привносяться потенційними загрозами та уразливостями. GLBA передбачає, що до реалізації програми в обов'язковому порядку повинні бути залучені керівні органи: рада директорів або інше вище керівництво. Обов'язковими компонентами програма є методика ефективного управління ризиками, моніторинг та внесення необхідних корегувань, а також звітність перед керівництвом. За GLBA звітність повинна передбачати розгляд, аналіз та рекомендації з наступних питань: *забезпечення контролю доступу; управління конфігураціями; виявлення шкідливих програм; забезпечення виконання вимог політики безпеки; моніторинг та управління правами користувачів; безпека інфраструктури та мереж передачі даних*.

На поточний момент чинність GLBA поширюється на банки, страхові компанії, брокерські фірми, податкові та бухгалтерські фірми, платіжні карткові системи та на ряд інших організацій, у відношенні кожної з яких існує відповідний регулятивний наглядовий орган: у США – це Комісія з цінних паперів та Федеральна корпорація страхування внесків. Відповідно до положень закону саме вони відповідають за перевірку (аудит) дотримання GLBA.

Наступний важливим закон США, що прямо стосуються конфіденційності та безпеки, є «Акт про медичне страхування» (*Health Insurance Portability and Accountability Act* – HIPAA) [6], затверджений у якості закону в 1996 році. Втім, багато з його положень, включаючи положення про конфіденційність персональних даних, були опубліковані набагато пізніше. Так, «Положення про конфіденційність персональних даних» та «Положення про безпеку» – у серпні 2002 та у лютому 2003 років, відповідно.

Основним стимулом прийняття HIPAA були не стільки ІБ та конфіденційність, скільки стандартизація інформації про стан здоров'я громадян США, якою обмінюються страхові компанії та медичні установи всієї країни. HIPAA, однак, вимагає від юридичних осіб, на яких поширюється його дія, прийняття розумних та належних фізичних, технічних і організаційних заходів безпеки, спрямованих на забезпечення цілісності та конфіденційності інформації про стан здоров'я фізичних осіб, яка перебуває в їхньому розпорядженні або передається ними партнерам. Такі ж заходи законом встановлюються до захисту від можливих загроз ІБ, несанкціонованого використання або розкриття даних клієнтів та до забезпечення дотримання вимог безпеки посадовими особами та службовцями. Це призвело до того, що вимоги HIPAA продумані більш детально, ніж вимоги британського GLBA, оскільки до прийняття HIPAA організації в сфері охорони здоров'я прикладали занадто мало зусиль для захисту конфіденційності інформації та часто продавали персональну інформацію третім сторонам (наприклад, фармацевтичним компаніям).

У цілому, при розробці організацією «Положення про безпеку», HIPAA вимагає від неї застосування уніфікованого підходу до захисту інформації як від внутрішніх, так і від зовнішніх загроз. У «Положенні…» організація повинна передбачити проведення систематичних, деталізованих та точних оцінок ризиків, а також містити цілком певні рекомендації у відношенні того, як це зробити.

Слід зазначити, що HIPAA є технологічно нейтральним законом, тобто він не пропонує характерних технічних розв'язків, що повинні підлягати впровадженню. Організації самі повинні демонструвати регуляторним органам, що вони забезпечують виконання положень закону або що вони у відповідній ситуації діяли розумним чином з метою дотримання вимог закону.

HIPAA також містить положення про регулярні перевірки на відповідність вимогам, однак порядок проведення таких перевірок, а також ким саме вони повинні проводитися, дотепер не уточнені.

Обговорення вимог в області аудиту ІБ, було б неповним без розгляду закону Сарбейнса-Окслі (*Sarbanes-Oxley Act* – SOX) [2], який був прийнятий у США у 2002 році.

SOX справив великий вплив на процес розвитку, впровадження та моніторинг систем

внутрішнього контролю компаній, включених у листинги бірж США. Спочатку прийнятий як реакція на великі скандали, пов'язані з шахрайством, як «спосіб захистити інвесторів за допомогою підвищення точності та вірогідності корпоративної інформації, що розкривається», закон мав велике значення для бізнесу та ІБ.

На ІБ організацій найбільший вплив справили статті 302 та 404 SOX. Так, стаття 302 передбачає, що головний виконавчий директор та головний фінансовий директор повинні особисто завіряти точність і повноту фінансових звітів. Більш того, вони повинні також оцінювати ефективність системи внутрішнього контролю відносно процесу формування фінансової звітності та представляти відповідні матеріали контролюючим органам. До цих матеріалів в обов'язковому порядку повинні включатися заходи контролю в області ІТ та ІБ. Стаття 404 регламентує, що компанії в обов'язковому порядку, крім перевірок контролюючими органами, повинні самостійно провадити оцінку ефективності системи внутрішнього контролю та повідомляти про результати оцінки Комісію з цінних паперів. У статті також передбачені вимоги до офіційних аудиторів компанії, які повинні оцінювати та вказувати у своєму висновку думку про ефективність системи внутрішнього контролю.

Т.ч., у SOX відзначаються наступні найважливіші вимоги до ІБ:

– за впровадження та функціонування системи внутрішнього контролю відносно процесу формування фінансової звітності відповідає керівництво компанії (організації);

– за результатами фінансового року керівництво компанії (організації) зобов'язане провести оцінку ефективності системи внутрішнього контролю;

– офіційні аудитори компанії повинні засвідчити самооцінку компанії (організації), та підготувати відповідний звіт.

Хоча провідні аудиторські фірми і раніше оцінювали систему внутрішнього контролю при перевірці фінансової звітності, SOX зробив цей процес більш точним, вимогливішим та обов'язковим. Як результат, зважаючи на SOX, аудиторські стандарти багатьох країн були переглянуті на предмет більш точного викладу процедур, заснованих на підході з точки зору ризиків та заходів контролю. У США це всі положення SOX розповсюджуються навіть компанії, які формально не підпадають під дію SOX. Очевидно, це пояснюється тим, що оцінка внутрішньої системи контролю не може бути здійснена без розгляду питань ІБ, за винятком, можливо, лише випадків, коли фінансові звіти та документи готуються без використання ІС.

Дія SOX не розповсюджується на незахищені системи, які ним розглядаються як джерела недостовірної фінансової інформації, що не має юридичної сили.

Для сприяння аудиторам в оцінці відповідності, згідно SOX, була створена Наглядова рада по фінансовій звітності публічних акціонерних товариств (*Public Company Accounting Oversight Board* – PCAOB) [7]. На PCAOB було покладене завдання розробки стандартів аудиту. Обрані PCAOB в якості базових типові заходи контролю, створені Комітетом фінансових організацій США (COSO) [8], забезпечують структуроване керівництво впровадженням системи внутрішнього контролю у всіх організаціях.

Хоча рамки COSO представляються гарною моделлю, все ж вони не дають достатньої інформації відносно супутніх засобів контролю в області ІТ та ІБ. У цьому зв'язку, на додаток до COSO, у США використовуються заходи контролю стандарту корпоративного управління та аудиту в області ІТ – COBIT. Стандарт розроблений Асоціацією по контролю та аудиту ІС (*Information Systems Audit and Control Association* – ISACA) [9]. Інститут ISACA по корпоративному управлінню в області ІТ (*IT Governance Institute* – ITGI) розробив на базі COSO та COBIT сукупність цільових заходів контролю в області ІТ та ІБ в контексті вимог SOX.

Хоча, як було зазначено вище, керівництво компанії має право прийняти розв'язок про використання іншої структури при розробці системи внутрішнього контролю, все ж це зажадає значних зусиль у плані розробки внутрішньої документації та обґрунтування того, чому обраний підхід відрізняється від рекомендованого ITGI. У зв'язку з цим, у найближчий час можна чекати, що компанії будуть дотримуватися рекомендацій ITGI для впровадження та оцінки заходів контролю в області ІТ та ІБ відповідно до вимог SOX.

На додаток до наведених прикладів законодавчого та регуляторного характеру в деяких галузях існують спеціальні вимоги, які організаціям необхідно виконувати. Так, у галузі платіжних карт обов'язковим є дотримання ряду стандартів та приписів, що є умовою випуску та процесингу карт різних брендів. На базі цього платіжна система Visa видала «Стандарти забезпечення безпеки даних при використанні платіжних карт» з обов'язковим мінімальним комплексом заходів щодо забезпечення ІБ. Подібно багатьом іншим регламентуючим приписам, згаданим вище, у них відсутні директиви відносно використання певних технологій, але є досить докладний перелік цілей контролю. Іншою відмінною рисою таких «корпоративних» стандартів є вимога про проведення регулярного зовнішнього аудиту на відповідність стандартам з використанням

спеціальної аудиторської програми. Відповідно до цього, аудит повинен проводитися кваліфікованою аудиторською компанією, що отримала акредитацію у повноважного органа платіжної системи (наприклад, Visa, Mastercard) на проведення таких перевірок.

Розглянуті міжнародні законодавчі акти, кожен з яких був розроблений з конкретною метою, не пов'язані безпосередньо з ІБ. Втім, всі вони вплинули на організацію та впровадження заходів з неї.

Крім зазначеного, слід відмітити, що вказані вище законодавчі акти ставляться до більшості організацій, для яких ІБ не є основним видом діяльності, а тільки засобом з захисту конфіденційності, цілісності та доступності інформації. Звичайно, винятком є випадки, коли організаціє є постачальником послуг в області ІБ.

Усі законодавчі акти, які розглянуті, об'єднані загальною метою: діяти «розумно» з погляду захисту інформації. Окремі акти мають більш жорсткий та розпорядчий характер, ніж інші, але жоден з них не визначає того, які технології повинні використовуватися або які конкретні засоби контролю повинна впровадити та реалізувати організація, щоб виконати вимоги законодавства. У цьому зв'язку дії аудиторів полягають у тому, щоб як можна більш гнучко підходити до питань тлумачення оцінки відповідності заходів контролю, впроваджених організацією, вимогам законодавства. Вітчизняні аудитори можуть заперечити, що ця невизначеність збільшує ризик: якби, наприклад, законодавчі акти чітко визначали, що всі страхові компанії зобов'язані мати міжмережеві екрани певного типу, настроєні встановленим та регламентованим чином, то тоді проводити аудит було б набагато простіше. Однак організації можуть бути зовсім не потрібними законодавчо регламентовані технології або можуть існувати вагомі комерційні причини, по яких їй необхідна інша конфігурація, яка жодним чином не піддає ризику загальний рівень безпеки.

Отже, гнучкість законів та регулятивних норм є позитивним чинником: вони встановлюють для організацій загальні рамки, у яких ті повинні діяти. Це не суперечить загальній фундаментальній правовій концепції «розумної необхідності», але залишає відкритим питання про те, що вважати розумно необхідним.

Дотримання розглянутих законодавчих актів може зажадати від організацій істотних витрат. Так, витрати, пов'язані з дотриманням вимог HIPAA, навіть у невеликих організаціях є значними, особливо з врахуванням того, що, наприклад, раніше вимог безпеки в галузі медичного страхування практично не було. Одна велика американська компанія, що займається медичним страхуванням, затратила більш 11 млн. доларів тільки на виплати консультантам для того щоб забезпечити дотримання вимог закону HIPAA. Компанії, що підпадають під дію SOX, витратили набагато більше, незважаючи на те, що складно сказати, яка частина цих коштів безпосередньо пов'язана з IT та ІБ: у кожному разі це чимала сума.

Аналогічно закони та регулятивні норми не враховують організаційні наслідки впровадження цих вимог. Що стосується SOX, то тут проведення організаційних змін неминуче. Так, по суті, всі акти, розглянуті вище, вимагають створення нових посад: офіцер по забезпеченню конфіденційності персональних даних, офіцер ІБ, аудитор безпеки і т.д. Разом з тим вони не дають достатньої інформації про те, які вимоги пред'являються до професійної підготовки та навичок таких співробітників, або нечітко визначають, які інші обов'язки можуть бути пов'язані з виконанням повноважень. Т.ч., на сьогодні залишається відкритим питання, де знайти відповідним чином підготовлений персонал та визначити його необхідну кваліфікацію. Крім того, неясно, як ефективно керувати людськими ресурсами, для того щоб забезпечити адекватний розподіл обов'язків. Це зворотний бік більшості будь-яких законодавчих актів: вони визначають загальні напрямки, але найчастіше ці загальні напрямки не дають відповіді на багато питань. За винятком актів, що регулюють діяльність у сфері випуску та процесінга платіжних карт, більшість законодавчих актів допускають велику кількість тлумачень: що таке «розумна необхідність», люди можуть розуміти по-різному. Усі законодавчі акти мають на увазі ту або іншу форму перевірки виконання вимог – або внутрішню перевірку, як у випадку з DPA у Великобританії, або зовнішню.

Складність проведення аудиту в розглянутих умовах віддаляє виконання вимог. Наприклад, неясно, хто повинен проводити перевірку дотримання вимог HIPAA та які цілі та основні області цієї перевірки. У найближчій перспективі компанії будуть залучати незалежних аудиторів здійснювати перевірки за типом «діагностики на відповідність вимогам». Це надасть їм можливостей продемонструвати законодавцям та регулювальним органам, що вони роблять все правильно до проведення офіційної аудиторської перевірки на відповідність. Знову виникає питання: як визначити часові рамки, характер та обсяг процедур проведення аудиту, якщо законодавчі та регулювальні органи не змогли самі цього зробити?

На Заході багато співробітників, що займають посади, пов'язані з забезпеченням ІБ в організаціях, ремствують, що вони не мають достатнього авторитету в організації, а коштів, які виділяються з бюджету, недостатньо для того, щоб забезпечити необхідний для бізнесу рівень безпеки. Найчастіше компанії не приділяють

достатню увагу ІБ, а зосереджені на поставлених виробничих завданнях і цілях, які іноді входять у суперечність з правилами дотримання безпеки.

У США під час буму електронної комерції відбулися певні позитивні зрушення в усвідомленні зв'язку цілей бізнесу та питань ІБ. Так, наприклад, належний рівень захищеності транзакцій через Інтернет став конкурентною перевагою. Але навіть «просунуті» компанії не змогли відповісти на два основні питання:

– Який рівень безпеки необхідний компанії?

– Як компанія може довести наявність необхідного рівня безпеки та належного контролю за ним?

Закони та регулятивні норми виявилися дуже корисними для підвищення статусу фахівців з безпеки, у яких зараз з'явилося право діяти. Вони можуть зробити *щось*, щоб забезпечити виконання вимог законодавства, і тому до думки таких фахівців керівництво компаній стало прислуховуватися. Особливо це ставиться до компаній, що підпадають під дію SOX, де вище керівництво несе карну відповідальність за недотримання закону. Як результат, ІБ в компаніях вийшла на новий рівень. Співробітники служби безпеки в даний момент перевантажені роботою з метою виконання вимог законодавства, не завжди розуміючи, як цього добитися, але принаймні тепер вони можуть звернутися до керівництва з вимогою збільшення фінансування.

Багато з розглянутих законів супроводжувалися раптовим сплеском фінансування на вдосконалювання ІБ та інших заходів контролю, але, можливо, у майбутньому така тенденція не збережеться. Проблемою залишається недостатній рівень зовнішнього аудиту на відповідність вимогам законодавства. Відповідно до цього, заходи щодо контролю дотримання нормативних актів є важливими для підтримки рівня ІБ, як пріоритетного завдання на рівні компанії.

З врахуванням того, що закони та нормативні акти дають можливість виявити тільки частину ситуації та вимагають від керівництва компанії діяти правильно, виникає питання, на яке необхідно відповісти: як виконуються вимоги законодавства і, що більш важливо, як можна довести, що ці вимоги виконуються? Усі законодавчі акти містять вимоги щодо проведення оцінки ризиків та розробки політики ІБ. У той же час тільки деякі з них пропонують, як повинна розроблятися політика безпеки, хто з керівництва повинен відповідати за її розробку та удосконалення і як ця політика повинна виконуватися. Фінансове та організаційне утримання політики ІБ у законодавстві освітлене тільки частково і чи навряд цього достатньо для того, щоб організація могла хоч що-небудь впровадити. З однієї сторони, це непогано: гнучкість у законодавстві означає, що організація може сама розробити політику ІБ, яка задовольняє її поточним і майбутнім потребам, а також відображає реальні умови, що існують в організації. Було б абсурдним, наприклад, пропонувати, щоб усі організації розробили політики відносно безпеки переносних комп'ютерів, якщо організація їх не використовує.

Звичайно, що тут на допомогу приходять стандарти. Більшість законодавчих актів розроблена з урахуванням консультацій, отриманих від різних органів по стандартизації. Стандарти в області ІТ та ІБ забезпечують управління наступним рівнем деталізації, який закони та нормативні акти не дають і не повинні давати.

Звичайно, стандарти не є обов'язковими та не встановлюються в законодавчому порядку, але вони дають керівництву можливість довести, що воно «діє належним чином» і в такий спосіб продемонструвати своє виконання вимог. Існує велика кількість стандартів в області ІТ та ІБ. Одні з них – галузеві, інші – загальні. Більшість з них засновані на оцінці ризиків, як невід'ємної частини процесу їх впровадження та дотримання. З врахуванням того, що закони та регулятивні акти також вимагають проведення оцінки ризиків при побудові системи внутрішнього контролю та забезпечення ІБ, це означає, що дотримання компанією вимог стандартів є першим правильним кроком на шляху виконання вимог законодавства.

Як вже зазначалося, у зв'язку з тим, що за кордоном існує безліч стандартів в області ІБ, організації нерідко зустрічаються з проблемою вибору найбільше для них підходящого. Оскільки для організацій, до яких пред'являються вимоги SOX, ITGI визначив підходящі заходи контролю в області ІТ та ІБ на основі стандарту COBIT, представляється, що їм має сенс починати з впровадження цього стандарту.

COBIT являє собою стандарт корпоративного управління ІТ, розроблений ISACA. Він адресований фахівцям в області ІТ, керівництву та аудиторам, і тому є корисним інструментом для організацій: допомагає керівництву та співробітникам зрозуміти необхідність контролю, а також дозволяє пояснити вимоги бізнесу технічним співробітникам.

COBIT розглядає корпоративне управління ІТ у рамках чотирьох основних груп процесів (доменів): організація та планування (PO); придбання та впровадження (AI); функціонування та підтримка (DS); моніторинг та оцінка (ME).

У кожному з вище приведених доменів виділяються окремі процеси (усього – 34). Для кожного з них приводяться вимоги до заходів контролю.

Серед процесів COBIT існує окремий процес, присвячений забезпеченню ІБ (DS5), хоча

й в інших процесах приводяться окремі заходи контролю, пов'язані з безпекою.

Відмінною рисою COBIT є наявність посібника з аудиту, що містить докладну методику перевірки заходів контролю по всіх 34 основних процесах IT, у т.ч. – по процесах, пов'язаних з безпекою. У керівництві докладно розповідається, з ким із співробітників необхідно провести опит та бесіду; які документи проаналізувати; що необхідно протестувати.

COBIT є корисним інструментом для внутрішніх та зовнішніх аудиторів. Він обумовлює підхід, за допомогою якого перевіряється рівень зрілості заходів контролю в області IT. Це робить його цінним інструментом для керівництва організації з метою визначення того, як « слід» діяти, і дозволяє сконцентрувати ресурси для вдосконалювання заходів контролю в тих областях, де потрібні поліпшення.

Після набрання чинності SOX усе більше уваги приділяється корпоративному управлінню, а значить, і управлінню IT та ІБ. Все більше організацій розглядають впровадження COBIT, як метод удосконалювання заходів контролю в області IT. Більше того, навіть безвідносно вимог SOX організації все частіше вимагають від незалежних консультантів проведення перевірок за вимогами COBIT для того, щоб оцінити ефективність корпоративного управління IT та, відповідно, ІБ.

Іншим корисним інструментом, який може використовуватися для вдосконалювання системи ІБ, є бібліотека інфраструктури IT (*IT Infrastructure Library* – ITIL) [10] – набір оптимальних методів та принципів, які визначають інтегрований, заснований на процесах підхід з управління IT. Зацікавленість у застосуванні ITIL постійно росте по усьому світу.

ITIL також рекомендує впровадження ефективних заходів в області ІБ на стратегічному, тактичному та операційному рівнях. Забезпечення ІБ розглядається як циклічний процес з фазами планування, впровадження, оцінки та підтримки. ITIL оперує такими поняттями в області ІБ, як *політики*, *процеси*, *процедури* та *інструкції*. З деякими особливостями аналогічні підходи прослідковуються в COBIT, а також у вітчизняних нормативних та законодавчих актах. Хоча в ITIL відсутні безпосередні спеціалізовані стандарти оцінки відповідності, він є близьким до британського стандарту BS 15000 [11], який присвячений управлінню IT-сервісами та методам їх оцінки.

Оцінку якості аудиторів, відповідно до BS 15000, здійснює Британське агентство акредитації (*United Kingdom Accreditation Service* – UKAS) [12]. UKAS встановлює основні вимоги відносно аудиторів у частині навчання, кваліфікації, наявності досвіду роботи у сертифікаційних компаній. Крім того, UKAS регулярно проводить аудит сертифікаційних компаній з метою переконатися, що вони можуть документально підтвердити свою компетентність по проведенню сертифікаційних аудитів. BS 15000 містить докладні керівництва для організацій, які бажали б отримати сертифікацію, і вимоги відносно аудиторів.

В 2005 році стандарт BS 15000 був представлений в ISO і по завершенню прискореної та спрощеної процедури він був прийнятий, як ISO/IEC 20000 [13].

Ще одним широко обговорюваним стандартом в області безпеки, є стандарт ISO/IEC 15408 «Загальні критерії ІБ IT» [14], який був гармонізований, наприклад, у Росії, як державний стандарт Р ИСО/МЭК 15408 [15]. Цей стандарт технічний і іноді важкий для сприйняття бізнесом. Він корисний для постачальників та покупців продукції ІБ, для того щоб визначити, наскільки достатнім є механізм захисту в продукції, що випробовується. На жаль, він не допомагає керівництву розібратися, чи правильно воно діє, забезпечуючи той чи інший рівень ІБ.

Область застосування ISO/IEC 15408 з метою відповідності регулюючим вимогам, є досить обмеженою. Однак існують виключення, зокрема в області процесінгу платіжних карт, де певні технічні вимоги стандарту зустрічаються, наприклад, у програмах перевірки на відповідність вимогам в області безпеки з боку платіжної системи Mastercard.

Найбільш відомими та широко використовуваними стандартами управління ІБ, а також доказом дотримання нормативних актів та законодавства, є міжнародні стандарти серії ISO/IEC 2700X по управлінню IT. Беручи свій початок від первісних Британських стандартів серії 7799 (далі – ISO/IEC 17799 [16] та ISO/IEC 27001 [17]), ці стандарти конкретно та чітко визначають технології ефективного впровадження систем управління IT. Є кілька причин, чому ці стандарти настільки популярні. Не останньою з них є та, що в них чіткі вказані методи проведення аудиторських перевірок на відповідність, а також можливість сертифікації по ISO/IEC 27001.

ISO/IEC 17799 та ISO/IEC 27001 допомагають відповістити на запитання: «як довести, що в організації забезпечений необхідний рівень безпеки?» і переконати регулювальні органі, що «усе виконується правильно» та « належним чином».

ISO/IEC 17799 та ISO/IEC 27001 охоплюють всі основні сфери вимог, які пропонуються законодавством та нормативними актами, згаданими вище. Наріжним каменем відповідності стандартам є розуміння того, які інформаційні активи має організація, і впровадження необхідного рівня заходів контролю, заснованого на оцінці ризиків.

ISO/IEC 17799 та ISO/IEC 27001 – це просто та доступно написані стандарти, що надають корисні методики з заходів контролю, які організація захоче впровадити. При цьому стандарти зрозумілі як фахівцям в області ІБ, так і керівництву. Вони допомагають подолати комунікаційний бар'єр між обома сторонами,

забезпечивши тим самим розуміння керівництвом, що робиться та чому. Керівництво розглядається стандартом як ключова ланка при постановці цілей в області ІБ.

Для того щоб бути сертифікованою по ISO/IEC 27001, організація повинна довести, що в неї існують процедури по ідентифікації законів та нормативних актів, що стосуються її з погляду захисту інформації. Крім того, у неї повинна існувати програма по дотриманню цих нормативних вимог. Тоді сертифікація по ISO/IEC 27001, якщо вона проведена належним чином, гарантувала б, що організація на ділі дотримує всі законодавчі та нормативні вимоги, які регулюють її діяльність.

Додаток А стандарту ISO/IEC 27001 містить перелік заходів контролю, які повинні бути впроваджені в організації, яка бажає пройти сертифікацію. Однак, слід зазначити, не всі заходи контролю з даного списку обов'язково повинні бути впроваджені, якщо з цього питання існує документально підтверджене рішення керівництва, засноване на оцінці ризиків. Багато компаній використовують ISO/IEC 27001 як засіб самооцінки, оскільки методик по проведенню оцінки безпеки недостатньо. Деякі компанії прагнуть пройти офіційний сертифікаційний аудит в акредитованих незалежних аудиторських організаціях. Аналогічно BS 15000, описаному вище, організації, які проводять сертифікаційний аудит, повинні бути акредитовані відносно стандарту BS 7799 (част. 2) органом UKAS у Великобританії. У міру приведення британських стандартів у статус міжнародних (ISO), акредитація також стає можливою через органи ISO.

В документі EA-7/3 «Акредитація організацій, що займаються сертифікацією систем управління ІБ» [18] Європейської комісії з акредитації, перераховані основні вимоги в області незалежності, кваліфікації та внутрішньої системи контролю якості відносно таких організацій. Ці вимоги до якості процесу сертифікації та кваліфікації аудиторів обумовлені необхідністю довіри до результатів сертифікації.

Сертифікація по стандартах також вимагає проведення регулярних аудиторських перевірок з метою забезпечення та підтримки відповідності виконання вимог, та для того, щоб процес управління безпекою функціонував належним чином. Це скорочує розрив, який у даний момент існує в більшості законодавчих актів: як довести регулювальним органам, що організація постійно дотримує вимог законодавства?

Сертифікація полегшує співробітникам служби безпеки отримання фінансування на підтримку програми управління безпекою, і не тільки на сам сертифікаційний аудит, але й на весь комплекс заходів в області безпеки.

У деяких країнах дотримання ISO/IEC 17799/BS 7799:2 у ряді галузей економіки є обов'язковим (наприклад, у Японії).

Регулювальні органі опираються на процес сертифікації по стандарту, як на достатню умову задоволення потреб галузі в захисті інформації. Можливо, інші країни будуть наслідувати цей приклад завдяки тому, що стандарт широко використовується як інструмент впровадження безпеки; він зрозумілий, а механізми його виконання (сертифікація) чітко встановлені.

Зазвичай, керівництво підприємства прагне знати, наскільки воно «розумно» діє в області ІБ. Керівництво також повинне могти забезпечити впровадження рішень, які б відповідали потребам бізнесу з погляду складності, організації робіт та витрат. Багато із законодавчих актів, яких необхідно дотримуватися, вимагають підходу, заснованого на оцінці ризиків, і не пропонують до застосування конкретні технології. Втім, інтуїтивно зрозумілим є той факт, що гарний стандарт не повинен пропонувати ту або іншу технологію або конкретні процедури контролю: він повинен бути досить гнучким, щоб дозволити будь-якій компанії дотримуватися вимог стандарту. Він повинен ґрунтуватися на оцінці ризику та повинен враховувати те, що завдання організації – це не забезпечення безпека, а ведення комерційної діяльності: у більшості випадків – заробляння грошей. Тому стандарт повинен забезпечувати гнучкість керівництву в прийнятті рішень, пов'язаних з безпекою, з урахуванням вимог бізнесу. Не все, що ризиковано, повинне бути заборонене: просто повинно бути більше різноманітних заходів контролю, що компенсують ризики. Т.ч., гарний стандарт повинен відображати потреби підприємств у розвитку.

Крім розглянутих, є й інші законодавчі акти: наприклад, такі, що стосуються злочинів по необережності. Так, якщо в компанії недостатні заходи контролю в області ІБ, внаслідок чого її комп'ютери були скомпрометовані та використовувалися для атаки проти третьої сторони, залишається питання про можливість судового позову третьої сторони проти компанії, що не приділила достатньої уваги питанням безпеки.

Висновок. Гарний стандарт в області аудиту інформаційної безпеки повинен давати спосіб вимірювати рівень відповідності йому, а також забезпечувати аудиторів (внутрішніх та зовнішніх) практичним інструментом оцінки безпеки та, як результат – вдосконалювати її. COBIT та серія стандартів ISO/IEC 2700X мають ці риси, що робить їхніми популярними як у бізнес-співтоваристві, так і серед фахівців в області безпеки.

Закони продовжують розроблятися та удосконалюватися. На сьогоднішній момент практичними діями щодо контролю за дотриманням вимог, а також визначенням, чи виконують організації всі можливі (чи необхідні) заходи з ІБ, є звернення до стандартів як способу довести, що вони діють належним чином.

Спостереження динамікою сертифікації як зарубіжних, так і вітчизняних організацій по ISO/IEC 27001 / BS 7799, показують, що цей процес буде тривати.

COBIT стає звичним терміном у лексиконі бізнесменів, а необхідність підходу до питань ІБ на основі оцінки ризику чітко усвідомлюється вищим керівництвом.

Керівники служб ІБ можуть отримувати фінансування, але вони повинні довести, що розумно витрачають кошти та використовують стандарти, як спосіб переконання керівництво в раціональності даного напрямку їх витрати.

Як остаточний підсумок: виконання стандартів є доказом того, що організація відповідально відноситься до пропонованих законодавства вимогами, хоча розуміє, що більшість законодавчих актів не пропонують технологій рішення всіх питань, а рекомендують керуватися здоровим глуздом.

Література

1. Аудит информационной безопасности предприятий и систем : навчальний посібник. – Тула : Московская академия комплексной безопасности. Тульский филиал, 2008. – 106 с. – ISBN відсутній.

2. Data Protection Act, 1998 [Електронний ресурс] // Портал : legislation.gov.uk. – Режим доступу \www/ URL : http://www.legislation.gov.uk/ukpga/1998/29/contents. – Заголовок з екрану, доступ вільний, 18.05.2013.

3. Закон Сарбэйнса-Оксли [Електронний ресурс] // Портал : Академик. – Режим доступу \www/ URL : http://dic.academic.ru/dic.nsf/ruwiki/923589. – Заголовок з екрану, доступ вільний, 18.05.2013.

4. The Computer Misuse Act [Електронний ресурс] // Портал : Teach-ICT. – Режим доступу \www/ URL : http://www.teach-ict.com/as_a2_ict_new/ocr/AS_G061/317_role_impact_ict/computer_misuse_act/miniweb/. – Заголовок з екрану, доступ вільний, 18.05.2013.

5. Gramm-Leach-Bliley Act of 1999 – GLBA [Електронний ресурс] // Портал : Investopedia. – Режим доступу \www/ URL : http://www.investopedia.com/terms/g/glba.asp. – Заголовок з екрану, доступ вільний, 18.05.2013.

6. Health Insurance Portability and Accountability Act [Електронний ресурс] // Портал : Wikipedia. – Режим доступу \www/ URL : http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act. – Заголовок з екрану, доступ вільний, 18.05.2013.

7. PCAOB oversees [Електронний ресурс] // Портал : PCAOB. – Режим доступу \www/ URL : http://pcaobus.org/Pages/default.aspx. – Заголовок з екрану, доступ вільний, 18.05.2013

8. Модель внутреннего контроля, ориентированная на оценку рисков [Електронний ресурс] // Портал : Образовательный сайт Мушкатовой Марии Сергеевны. – Режим доступу \www/ URL : http://myshkatova.ru/page141/page157/index.html. – Заголовок з екрану, доступ вільний, 18.05.2013.

9. About ISACA [Електронний ресурс] // Портал : ISACA. – Режим доступу \www/ URL : http://www.isaca.org/about-ISACA/Pages/default.aspx. – Заголовок з екрану, доступ вільний, 18.05.2013.

10. Бібліотека IT-інфраструктури [Електронний ресурс] // Портал : MCUa. – Режим доступу \www/ URL : http://www.management.com.ua/glossary/thesaurus.php?id=165. – Заголовок з екрану, доступ вільний, 18.05.2013.

11. The ISO 20000 (BS15000/BS15000) ITSM Standard [Електронний ресурс] // Портал : The ISO 20000 Directory. – Режим доступу \www/ URL : http://www.bs15000.org.uk/. – Заголовок з екрану, доступ вільний, 18.05.2013.

12. About UKAS [Електронний ресурс] // Портал : UKAS. – Режим доступу \www/ URL : http://www.ukas.com/about-accreditation/about-ukas/. – Заголовок з екрану, доступ вільний, 18.05.2013.

13. О стандарте ISO/IEC 20000 [Електронний ресурс] // Портал : TMS Ukraine. More than only certification. – Режим доступу \www/ URL : http://tms-ua.com/system-management/ iso-20000/. – Заголовок з екрану, доступ вільний, 18.05.2013.

14. Общие критерии оценки безопасности информационных технологий [Електронний ресурс] // Портал : ISO27000.ru. – Режим доступу \www/ URL : http://www.iso27000.ru/ standarty/iso-15408-obschie-kriterii-ocenki-bezopasnosti-informacionnyh-tehnologii. – Заголовок з екрану, доступ вільний, 18.05.2013.

15. Руководящий документ «Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности» [Електронний ресурс] // Портал : sakha.gov. – Режим доступу \www/ URL : http://sakha.gov.ru/SbornikNPA/FSTEK.files/doc_3_3_012.htm. – Заголовок з екрану, доступ вільний, 18.05.2013.

16. International Standard ISO/IEC FDIS 17799:2005 [Електронний ресурс] // Портал : rutracker.org. – Режим доступу \www/ URL : http://rutracker.org/forum/viewtopic.php?t= 702233. – Заголовок з екрану, доступ вільний, 18.05.2013.

17. Система менеджмента информационной безопасности по требованиям международного стандарта ISO/IEC 27001:2005 [Електронний ресурс] // Портал : TÜV NORD. – Режим доступу \www/ URL : http://www.tuev-nord.com.ua/index.php/sertsm/isoiec-27001. – Заголовок з екрану, доступ вільний, 18.05.2013.

18. МСЗБП: 6.3. Правові основи аудиту систем менеджменту : документ ЕА-7/3 [Електронний ресурс] // Портал : Віртуальне Навчальне Середовище Львівської Політехніки. – Режим доступу \www/ URL : http://www.google.com.ua/url?sa=t&rct=j&q=%22%D0%B5%D0 %B0-7%2F3%22&source=web&cd=6&cad=rja&ved=0CEgQFjAF&url=http%3A%2F%2Fvns.lp.edu.ua%2Fmoodle%2Fmod%2Fpage%2Fview.php%3Fid%3D90925&ei=q1UKUp6aLa2w4QS3o4DoDg&usg=AFQjCNH-GObGkQX2MwkKJ4CSt_4G4pgVYg&bvm=bv.50500085,d.bGE. – Заголовок з контейнера, доступ по паролю, 18.05.2013.

References

1. Audit informacionnoj bezopasnosti predprijatij i sistem : navchal'nij posibnik. – Tula : Moskovskaja akademija kompleksnoj bezopasnosti. Tul'skij filial, 2008. – 106 s. – ISBN vidsutnij.

2. Data Protection Act, 1998 [Elektronnij re¬surs] // Portal : legislation.gov.uk. – Rezhim dos¬tupu \www/ URL : http://www.legislation.gov.uk/ukpga/1998/29/contents. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

3. Zakon Sarbjejnsa-Oksli [Elektronnij re¬surs] // Portal : Akademik. – Rezhim dos¬tupu \www/ URL : http://dic.academic.ru/dic.nsf/ruwiki/923589. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

4. The Computer Misuse Act [Elektronnij re¬surs] // Portal : Teach-ICT. – Rezhim dos¬tupu \www/ URL :

http://www.teach-ict.com/as_a2_ict_new/ocr/AS_G061/317_role_impact_ict/computer_misuse_act/miniweb/. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

5. Gramm-Leach-Bliley Act of 1999 – GLBA [Elektronnij re¬surs] // Portal : Investopedia. – Rezhim dos¬tupu \www/ URL : http://www.investopedia.com/terms/g/glba.asp. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

6. Health Insurance Portability and Accountability Act [Elektronnij re¬surs] // Portal : Wikipedia. – Rezhim dos¬tupu \www/ URL : http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

7. PCAOB oversees [Elektronnij re¬surs] // Portal : PCAOB. – Rezhim dos¬tupu \www/ URL : http://pcaobus.org/Pages/default.aspx. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013

8. Model' vnutrennego kontrolja, orientirovannaja na ocenku riskov [Elektronnij re¬surs] // Portal : Obrazovatel'nyj sajt Mushkatovoj Marii Sergeevny. – Rezhim dos¬tupu \www/ URL : http://myshkatova.ru/page141/page157/index.html. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

9. About ISACA [Elektronnij re¬surs] // Portal : ISACA. – Rezhim dos¬tupu \www/ URL : http://www.isaca.org/about-ISACA/Pages/default.aspx. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

10. Biblioteka IT-infrastrukturi [Elektronnij re¬surs] // Portal : MCUa. – Rezhim dos¬tupu \www/ URL : http://www.management.com.ua/glossary/thesaurus.php?id=165. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

11. The ISO 20000 (BS15000/BS15000) ITSM Standard [Elektronnij re¬surs] // Portal : The ISO 20000 Directory. – Rezhim dos¬tupu \www/ URL : http://www.bs15000.org.uk/. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

12. About UKAS [Elektronnij re¬surs] // Portal : UKAS. – Rezhim dos¬tupu \www/ URL : http://www.ukas.com/about-accreditation/about-ukas/. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

13. O standarte ISO/IEC 20000 [Elektronnij re¬surs] // Portal : TMS Ukraine. More than only certification. – Rezhim dos¬tupu \www/ URL : http://tms-ua.com/system-manage¬ment/ iso-20000/. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

14. Obshhie kriterii ocenki bezopasnosti informacionnyh tehnologij [Elektronnij re¬surs] // Portal : ISO27000.ru. – Rezhim dos¬tupu \www/ URL : http://www.iso27000.ru/ standarty/iso-15408-obschie-kriterii-ocenki-bezopasnosti-informacionnyh-tehnologii. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

15. Rukovodjashhij dokument «Bezopasnost' informacionnyh tehnologij. Polozhenie po razrabotke profilej zashhity i zadanij po bezopasnosti» [Elektronnij re¬surs] // Portal : sakha.gov. – Rezhim dos¬tupu \www/ URL : http://sakha.gov.ru/SbornikNPA/FSTEK.files/doc_3_3_012.htm. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

16. International Standard ISO/IEC FDIS 17799:2005 [Elektronnij re¬surs] // Portal : rutracker.org. – Rezhim dos¬tupu \www/ URL : http://rutracker.org/forum/viewtopic.php?t= 702233. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

17. Sistema menedzhmenta informacionnoj bezopasnosti po trebovanijam mezhdunarodnogo standarta ISO/IEC 27001:2005 [Elektronnij re¬surs] // Portal : TÜV NORD. – Rezhim dos¬tupu \www/ URL : http://www.tuev nord.com.ua/index.php/sertsm/isoiec-27001. – Zagolovok z ekranu, dostup vil'nij, 18.05.2013.

18. MSZBP: 6.3. Pravovi osnovi auditu sistem menedzhmentu : dokument EA-7/3 [Elektronnij re¬surs] // Portal : Virtual'ne Navchal'ne Seredovishhe L'vivs'koï Politehniki. – Rezhim dos¬tupu \www/ URL : http://www.google.com.ua/url?sa=t&rct=j&q=%22%D0%B5%D0 %B0-7%2F3%22&source=web&cd=6&cad=rja&ved=0CEgQFjAF&url=http%3A%2F%2Fvns.lp.edu.ua%2Fmoodle%2Fmod%2Fpage%2Fview.php%3Fid%3D90925&ei=q1UKUp6aLa2w4QS3o4DoDg&usg=AFQjCNH-GObGkQX2MwkKJ4CSt_4G4pgVYg&bvm=bv.50500085,d.bGE. – Za¬golovok z kontejnera, dostup po parolju, 18.05.2013.

Казакова Н.Ф., Плешко Э. А., Айвазова К. Б.

МЕЖДУНАРОДНАЯ РЕГЛАМЕНТАЦИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ И СТАНДАРТИЗАЦИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье, опираясь на зарубежные публикации, проведен обзор нормативных и законодательных документов, регулирующих технологии аудита информационной безопасности организаций. Показано, что законы продолжают разрабатываться и совершенствоваться. Определено, что актуальным вопросом являются требования к практическим действия со стороны организаций по контролю за соблюдением требований к информационной безопасности. Отмечено, что актуальным вопросом является порядок определения, выполняют ли организации все необходимые меры по информационной безопасности.

Ключевые слова: *DPA, CMA, GLBA, HIPAA. SOX, COSO, COBIT, ITIL, BS 15000, ISO/IEC 20000, ISO/IEC 15408, Р ИСО/МЭК 15408, ISO/IEC 17799, ISO/IEC 27001, EA-7/3.*

Kazakova N.F., Pleshko E. A., Aivazova K.B.

INTERNATIONAL REGULATION OF REGULATORY OF DOCUMENTS AS WELL STANDARDIZATION IN AREA AUDIT OF INFORMATION SECURITY

An overview of the regulatory and legislative instruments that regulate the audit of information technology security. It is shown that the laws continue to be developed and improved. An assessment of whether the practical actions of organizations to monitor compliance with the requirements for information security. Examines the question of how to perform the necessary steps organizations on information security.

Keywords: *DPA, CMA, GLBA, HIPAA. SOX, COSO, COBIT, ITIL, BS 15000, ISO/IEC 20000, ISO/IEC 15408, ISO/IEC 15408, ISO/IEC 17799, ISO/IEC 27001, EA-7/3.*

Надія Феліксівна Казакова – доцент кафедры Информационных систем в экономике, кандидат технических наук, доцент, Одесский национальный экономический университет

Плешко Едуард Анатолійович – старший науковий співробітник, кандидат юридичних наук, Український науково-дослідний інститут медицини транспорту

Айвазова Кіра Борисівна – здобувач кафедри Інформаційно-вимірювальних технологій, Одеська державна академія технічного регулювання та якості

Рецензент: Петров Олександр Степанович – докт. техн. наук, професор, завідувач кафедри безпеки інформаційних систем, Східноукраїнський національний університет імені Володимира Даля, м. Луганськ.