МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Сучасні технології у промисловому виробництві

М А Т Е Р І А Л И
т а п р о г р а м а

ІІІ Всеукраїнської міжвузівської науково-технічної конференції (Суми, 22–25 квітня 2014 року)

ЧАСТИНА 1

Конференція присвячена Дню науки в Україні

Суми
Сумський державний університет
2014

СТАНДАРТИ В ГАЛУЗІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Залога В. О., професор, Івченко О. В., докторант,
Янченко В. М., аспірант, СумДУ, м. Суми

Основою міжнародних стандартів (МС) управління інформаційною безпекою є серія британських стандартів BS 7799. Стандарт BS 7799-1 «Практичні правила управління інформаційною безпекою» – був розроблений в 1995 р. і є практичним посібником з управління інформаційною безпекою в організації. Він регламентує 10 областей і 127 механізмів контролю, необхідних для побудови системи управління інформаційної безпеки (СУІБ).

У 1998 році з'явилася друга частина цього британського стандарту – BS 7799-2 «Системи управління інформаційною безпекою. Специфікація і керівництво щодо застосування», що визначила загальну модель побудови СУІБ і набір обов'язкових вимог з сертифікації. З появою другої частини BS 7799, що визначила, що повинна з себе представляти СУІБ, почався активний розвиток системи сертифікації в галузі управління безпекою. У 1999 році обидві частини BS 7799 були переглянуті і гармонізовані з МС систем управління ISO 9001 та ISO 14001, а рік потому технічний комітет ISO без змін прийняв BS 7799-1 в якості МС ISO 17799, який згодом був перейменований в ISO 27002.

Основною перевагою ISO 17799 та споріднених йому стандартів є їх гнучкість й універсальність. Описаний в ньому набір кращих практик застосуємо практично до будь-якої організації, незалежно від форми власності, виду діяльності, розміру і зовнішніх умов. Він нейтральний в технологічному плані й завжди залишає можливість вибору технологій.

У МС серії ISO 27000 знайшло відображення все, що потрібно для управління інформаційними ризиками. Йдеться насамперед про МС ISO 27001:2005 з виходом якого СУІБ придбали міжнародний статус, і тепер роль і престижність СУІБ, що пройшли процедуру підтвердження (сертифікації) на відповідність вимогам МС ISO 27001, значно підвищився. А також про прийнятий у 2008 році МС ISO 27005 і його попередник – британський стандарт BS 7799-3:2006, які в багатьох речах взаємно дублюють, а в деяких питаннях доповнюють один одного.

Всупереч очікуванням, ISO 27005 зовсім не є міжнародною версією BS 7799-3, на відміну від своїх попередників ISO 27001 та ISO 27002, які, як відомо, є міжнародними версіями британських стандартів BS 7799-2 і BS 7799-1 відповідно. ISO 27005 прийшов на зміну МС ISO 13335-3 та ISO 13335-4, дія яких тепер скасовано. Це свідчить про позитивний процес заміщення вже злегка застарілої серії стандартів IT безпеки ISO 13335 щодо нової серії стандартів у галузі управління інформаційною безпекою

ISO 27000. У результаті цього процесу стандартів стає менше, а їх якість помітно поліпшується.

Заслуговує також згадки американський стандарт в галузі управління ризиками NIST 800-30, який, у свою чергу, спирається на ISO Guide 73, ISO 16085 та AS/NZS 4360. Основні положення цього стандарт були враховані при розробці ISO 27005.

Зіставляючи стандарти BS 7799-3 та ISO 27005, можна зробити висновок, що вони визначають найбільш важливі моменти, пов'язані з ризиками, схожими шляхами. Це стосується процесної моделі, елементів управління ризиками, підходів щодо аналізу ризиків і способам їх обробки, а також питань комунікації ризиків. Обидва стандарти містять у вигляді додатків приклади типових загроз, вразливостей і вимог безпеки.

Однак різні джерела розробки зумовили й ряд відмінностей між британським і МС управління ризиками. ISO 27005 більш докладно описує критерії та підходи щодо оцінки ризиків, контекст управління ризиками, область і межі оцінки, а також обмеження, що впливають на зменшення ризику. Водночас BS 7799-3 більш тісно пов'язаний з ISO 27001 і безпосереднім чином відображає процеси управління ризиками на процеси життєвого циклу СУІБ. Він також визначає вимоги до експерта з оцінювання ризиків та ризик-менеджеру і включає в себе рекомендації з вибору інструментарію для оцінки ризиків. BS 7799-3 також містить приклади законодавчих і нормативних вимог стосовно США та країн Європи.