УДК 004.056:006.42

Гуз А. М.
Національний педагогічний університет
імені М. П. Драгоманова

СТАНОВЛЕННЯ ТА РОЗВИТОК СВІТОВИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

У статті охарактеризований процес становлення та розвитку світових стандартів інформаційної безпеки з 80-х років XX ст. до першого десятиліття XXI ст.

Ключові слова: *стандарти, інформаційна безпека.*

Жодне суспільство не може існувати без законодавства та нормативних документів, які регламентують правила, процеси, методи виготовлення та контролю якості товарів, робіт і послуг, а також гарантують безпеку життя, здоров'я і майна людей та навколишнього середовища. Стандартизація якраз і є тією діяльністю, якій притаманні ці функції.

Стандартизація – діяльність, що полягає у встановленні положень для загального і багаторазового застосування щодо наявних чи можливих завдань з метою досягнення оптимального ступеня впорядкування у певній сфері, результатом якої є підвищення ступеня відповідності продукції, процесів та послуг їх функціональному призначенню, усуненню бар'єрів у торгівлі і сприянню міжнародному співробітництву.

Об'єктом стандартизації є продукція, процеси та послуги, зокрема матеріали, приміщення, обладнання, системи, їх сумісність, правила, процедури, форми методи чи взагалі діяльність.

Метою стандартизації в сучасному світі є забезпечення безпеки життя та здоров'я людини, тварин, рослин, а також майна та охорони довкілля, створення умов для раціонального використання всіх видів національних ресурсів та відповідності об'єктів стандартизації своєму призначенню, сприяння усуненню технічних бар'єрів у торгівлі.

Метою статті є характеристика процесу становлення та розвитку світових стандартів інформаційної безпеки.

Аналіз останніх досліджень і публікацій свідчить, що українські вчені значну уваги приділяють цьому питанню, підтверджуючи беззаперечну його актуальність. Переважна більшість зарубіжних та українських дослідників основну увагу приділяють висвітленню теоретичних основ стандартів інформаційної безпеки. Процес становлення та розвитку світових стандартів інформаційної безпеки лишався поза увагою науковців. Варто зазначити й про останні фундаментальні праці з цієї проблеми К. Белякова [1], Н. Кушакової-Костицької [2], Л. Задорожньої [3], В. Сідака [4], В.Артемова [5] О. Богданова, О. Бакалинського [6] та інших.

Європейська політика у сфері стандартизації базується на таких принципах: забезпечення участі фізичних і юридичних осіб у розробленні стандартів та у вільному виборі ними видів стандартів при виробництві чи постачанні продукції; відкритість та прозорість процедур розроблення та прийняття стандартів з урахуванням інтересів усіх зацікавлених сторін, підвищення конкурентоспроможності продукції вітчизняних виробників; доступність стандартів та інформації щодо них для користувачів;

відповідність стандартів законодавству; адаптація до сучасних досягнень науки і техніки з урахуванням стану національної економіки; пріоритетність прямого впровадження в країнах Європи, міжнародних та регіональних стандартів; дотримання міжнародних та європейських правил і процедур стандартизації;

Суб'єктами стандартизації є: центральний орган виконавчої влади у сфері стандартизації; рада стандартизації; інші суб'єкти, що займаються стандартизацією.

Застосування стандартів є обов'язковим для: всіх суб'єктів господарювання, якщо це передбачено в технічних регламентах чи інших нормативно-правових актах; учасників угоди (контракту) щодо розроблення, виготовлення чи постачання продукції, якщо в ній (ньому) є посилання на певні стандарти; виробника чи постачальника продукції, якщо він склав декларацію про відповідність продукції певним стандартам чи застосував позначення цих стандартів у її маркуванні; виробника чи постачальника, якщо його продукція сертифікована щодо дотримання вимог стандартів .

У 1947 році була створена Міжнародна організація зі стандартизації (International Standards Organization, скорочена назва – ISO), штаб-квартира в Женеві. Першочерговою її метою було створення лише системи стандартів, які б сприяла міжнародній торгівлі. Більшість країн світу мають національні представництва та національні комітети в ISO.

В своїй діяльності ISO взаємодіє з іншими міжнародними організаціями зі стандартизації. В галузі інформаційної безпеки такою організацією є IEC – Міжнародна електротехнічна комісія, котра була створена ще в 1906 р., метою її є встановлення міжнародних стандартів у всіх галузях, пов'язаних з електрикою, електронікою та радіотехнікою.

Міжнародною організацією зі стандартизації прийнято низку стандартів, які діють у Європейському співтоваристві. Основні з них: ISO 9000, ISO 9001, ISO 9004 (менеджмент якості); ISO 10001, ISO 10002, ISO 10003, ISO 10004 (задоволеність споживачів); EN 9100 (СМК в аерокосмічній галузі); ISO/TS 16949 (СМК в автомобілебудуванні); ISO 14001 (екологічний менеджмент); OHSAS 18001 (професійна безпека); ISO 31000 (менеджмент ризиків); ISO 20000 (СМК IT- послуг); ISO 22000 (продовольча безпека); ISO 26000 (соціальна відповідальність); ISO 50000 (системи менеджменту в енергетиці); ISO 27001 (інформаційна безпека).

Перші стандарти інформаційної безпеки були розроблені на початку 80-х років 20 ст. В першу чергу вони стосувалися інформаційної безпеки ПЕОМ.

Перший стандарт безпеки – "Orange book" (1983 р.) насамперед призначався для системи військового комплексу, він був заснований виключно на мейнфреймах, і його адаптація для розподільних систем та баз даних потребувала розробки додаткових документів.

"Європейські критерії" (1986 р.) значно ґрунтовніший документ, на рівні базового документа в цей стандарт увійшли розподілені системи, мережі, системи телекомунікацій.

Керівні "Документи ГКТ"(1992 р.) за конкретністю своїх вимог перевищили рівень "Orange book", оскільки детально регламентують реалізацію функцій захисту (це єдиний стандарт, котрий в ультимативній формі вимагає використання криптографії).

"Федеральні критерії"(1992 р.) підняли галузь застосування стандартів на новий рівень, розпочали розглядати інформаційні технології, незалежно від їх призначення, проводячи розходження тільки характеристиками середовища їх експлуатації.

"Канадські критерії"(1993 р.) характеризують галузь застосування усі типи комп'ютерних систем.

"Єдині Критерії" (1996 р.) увінчали процес розширення сфери застосування стандартів інформаційної безпеки, стали невід'ємним компонентом інформаційних технологій.

Головне завдання стандартів інформаційної безпеки 80-90 років 20 ст. – узгодженість позицій та запитів виробників, споживачів і аналітиків класифікаторів продуктів інформаційних технологій.

У якості загальних показників, стандарти які характеризують інформаційну безпеку фахівці називають такі: універсальність, гнучкість, гарантованість, реалізація та актуальність.

З огляду на це в таблиці представлені якісні характеристики перших стандартів інформаційної безпеки.

Стандарти безпеки	***Якісні характеристики стандартів інформаційної безпеки***				
	Універсальність	***Гнучкість***	***Гарантованість***	***Реалізація***	***Актуальність***
"Orange book" (1983 р.)	обмежена	обмежена	обмежена	скромна	помірна
"Європейські критерії" (1986 р.)	помірна	помірна	помірна	висока	помірна
"Документи ГКТ"(1992 р.)	обмежена	обмежена	відсутня	висока	обмежена
"Федеральні критерії" (1992 р.)	висока	відмінна	достатня	висока	висока
"Канадські критерії" (1993 р.)	помірна	достатня	достатня	достатня	середня
"Єдині Критерії" (1996 р.)	чудові	чудові	чудові	чудові	чудові

Найбільш повно критерії для оцінки механізмів безпеки програмно-технічного рівня представлені в міжнародному стандарті ISO 15408: Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінки безпеки інформаційних технологій), прийнятому в 1999 році.

Загальні критерії оцінки безпеки інформаційних технологій ("Загальні критерії") визначають функціональні вимоги безпеки (security functional requirements) і вимоги до адекватності реалізації функцій безпеки (security assurance requirements).

Хоча застосовність "Загальних критеріїв" обмежується механізмами безпеки програмно-технічного рівня, в них міститься певний набір вимог до механізмів безпеки організаційного рівня і вимог з фізичного захисту, які безпосередньо пов'язані з описаними функціями безпеки.

Ключовим міжнародним стандартом з безпеки інформації є розроблений Міжнародною організацією стандартів (International Standards Organization, ISO)

ISO/IEC 17799:2000 Information Security Management Standard (Code of Practice for Information Security Management) – зведення правил і норм управління безпекою в галузі інформаційних технологій [5]. ISO 17799 містить практичні правила з управління інформаційною безпекою і може використовуватися в якості критеріїв для оцінки механізмів безпеки організаційного рівня, включаючи адміністративні, процедурні та фізичні заходи захисту.

Варто зазначити, що зазначений стандарт бере свій початок з 90-х років XX ст. Саме в середині 90-х років Британський інститут стандартів (BSI) за участі комерційних організацій, таких як Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks & Spencer, Logica та ін., зайнявся розробкою стандарту управління інформаційною безпекою, в 1995 р. був прийнятий національний британський стандарт BS 7799 (Практичні правила управління інформаційною безпекою) з управління інформаційною безпекою та її організації незалежно від сфери діяльності.

Перша частина стандарту носила рекомендаційний характер, а друга булла призначена для сертифікації та містила частину обов'язкових вимог, що не входили в першу частину.

У 1999 році була опублікована друга частина стандарту: BS 7799 частина 2 "Системи управління інформаційною безпекою – Специфікація та керівництво щодо застосування" (Системи управління інформаційною безпекою – специфікації з керівництвом з використання). На його базі був "зроблений стандарт ISO / IEC 27001:2005 "Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги", на відповідність якому може проводитися сертифікація.

Як і будь-який національний стандарт, BS 7799 у період 1995-2000 рр. користувався помірною популярністю лише в рамках: країн британської співдружності.

Наприкінці 1999 р. експерти Міжнародної організації зі стандартизації ISO дійшли висновку, що в рамках існуючих стандартів ISO відсутній спеціалізований стандарт управління інформаційною безпекою. Відповідно, ISO було ухвалене рішення не починати розробку нового стандарту, а узгодивши із Британським інститутом стандартів, прийняти стандарт ISO 17799 на базі BS 7799:1.

Саме тому в 2000 р. BS 7799:1 став ISO 17799, одержав вже статус міжнародного стандарту, що значно змінило відношення до стандарту.

Цей стандарт регламентує такі аспекти: планування послідовності дій; контроль за доступом до системи; побудова та обслуговування систем; відповідність вимогам; захист особистої інформації; захист інформації, що належить організації; управління комп'ютерним забезпеченням та мережами; класифікація IT-активів та контроль за ними; політика захисту даних.

У середині 2001 р. у світі існували різні точки зору на стандартизацію з інформаційної безпеки. Існували різні стандарти, застосування яких на практиці викликало питання та серйозні сумніви. Крім того, у більшості фахівців переважав винятково технологічний підхід до захищеності (тобто визнавалися лише технічні методи захисту), а питанням організаційно-правового управління безпекою приділялася мінімальна увага.

До кінця 2002 р. у світі існувало 150 компаній, що мали сертифікат BS 7799 [6].

З 2003 р. зростання інтересу фахівців і представників бізнесу до ISO 17799. За рік збільшується кількість компаній у світі, що одержали офіційний сертифікат – до 1000. Таке значне зростання числа сертифікованих компаній у 2004 р. пояснюється тим, що саме цей рік показав тенденцію загального практичного інтересу до стандарту у світі й країнах СНД. У Росії, Казахстані, Молдові, Узбекистані, Україні – стандарт став повсюдно застосовуватися на практиці (або прийшло усвідомлення необхідності його застосування як кращої світової практики).

В останнє десятиліття європейські країни впроваджують ISO 17799. У Росії ISO 17799 став Держстандартом. Прийняття Держстандарту 17799 відбулося в 2006 р.

В наш час стандарт ISO 17799 використовують для побудови систем управління інформаційною безпекою провідних компаній як в Європі та Азії, так і в країнах СНД.

У 2005 році вийшла нова о редакція стандарту ISO 17799:2005 – сертифікаційний стандарт ISO 27001. У 2007 році ISO 17799 було пере опрацьовано і перевидано під номером ISO / IEC 27002.

Основний зміст стандарту зберігся, але багато що було повністю перероблене, щоб краще відповідати новим інформаційним загрозам і викликам безпеки.

ISO 17799:2007 (ISO / IEC 27002) складається з 13 розділів: загальна частина; терміни та визначення; політика безпеки; організаційні методи забезпечення інформаційної безпеки; управління ресурсами; користувачі інформаційної системи; фізична безпека; управління комунікаціями та процесами; контроль доступу; придбання, розробка та супровід інформаційних систем; управління інцидентами інформаційної безпеки; управління безперервністю ведення бізнесу; відповідність вимогам.

ISO/IEC 17799:2007 (ISO / IEC 27002) призначений для використання будь-якою організацією, яка дбає про належну систему ефективного інформаційного захисту або хоче поліпшувати існуючі методи інформаційного захисту [6].

Таким чином охарактеризований процес становлення та розвитку світових стандартів інформаційної безпеки з 80-х років XX ст. до першого десятиліття XXI ст. З'ясовано еволюцію світової стандартизації у сфері інформаційної безпеки. Зазначимо, що стандарти з інформаційної безпеки містить у собі рекомендації з управління інформаційною безпекою, призначені для співробітників, відповідальних за створення, впровадження й підтримку заходів, які забезпечують безпеку на державному підприємстві або недержавній організації. Рекомендації, наведені в стандартах інформаційної безпеки, використовують з урахуванням національних законів і нормативних вимог. Вже сьогодні міжнародні стандарти інформаційної безпеки все більше стають основою для розробки стандартів безпеки й ефективних методів управління інформаційною безпекою в конкретній організації, на підприємстві, в установі.

В и к о р и с т а н і д ж е р е л а :

1. *Беляков К.* Інформатизація організаційно-правової сфери суспільної діяльності // Право України. – 2004. – № 6. – С. 88-92.
2. *Кушакова-Костицька Н.* Від свободи слова до інформаційного суспільства // Право України. – 2004. – № 7. – С. 129-133.

3. *Задорожня Л.* До питання огляду законодавства в інформаційній сфері // Правова інформатика. – 2004. –№ 3. – С. 18-23.
4. *Сідак В.*
5. *Артемов В.* Міжнародний стандарт ISO 17799 як складова в галузі менеджменту інформаційної безпеки // Юридичний журнал "ЮСТИНІАН" № 11 / 2007 [Електронний ресурс]. − Режим доступу: http://www.justinian.com.ua/article.php?id=2802
6. *Богданов О., Бакалинський О.* "Адаптація міжнародного стандарту управління інформаційною безпекою ISO / IEC 27001:2005у структурах державного управління України". [Електронний ресурс]. – Режимдоступу:http://nc.nusta.com.ua/Kyrsi%202009/tezi/images_tezi/S_6_Bogdanov_Bakalynsky_1.htm.
7. Анализ международного стандарта ISO 15408 : информационная технология, методы и средства // Бизнес и безопасность. – 2007. – №561.

Гуз А. М. Становление и развитие мировых стандартов информационной безопасности.

В статье охарактеризованный процесс становления и развития мировых стандартов информационной безопасности с 80-х годов XX ст. по первое десятилетие XXI ст.

Ключевые слова: *стандарты, информационная безопасность*

Guz A. M. Emergence and development of world standards of information security.

The article described the process of formation and development of international standards of information security from the 80 years of the twentieth century. for the first decade of the XXI century.

Keywords: *standards, information security.*

КОНСТИТУЦІЙНЕ ПРАВО

УДК 34(09)"19/20":351

Єфремова О. П.
Національний педагогічний університет
імені М. П. Драгоманова

КОНКУРС ЯК РІЗНОВИД КАДРОВОЇ ПРОЦЕДУРИ ПРИ ФОРМУВАННІ КАДРОВОГО ПОТЕНЦІАЛУ ДЕРЖАВНОЇ СЛУЖБИ УКРАЇНИ

У статті досліджуються теоретичні проблеми порядку проведення конкурсу на заміщення вакантних посад державних службовців. Зокрема, акцентується увага на визначенні конкурсу як різновиду кадрової процедури при формуванні кадрового потенціалу державної служби України та дослідженні конкурсу у процесі формування кадрового потенціалу державної служби.

Ключові слова: *кадрова процедура, кадровий потенціал, заміщення, вакантна посада, конкурс, державна служба.*

Ефективність діяльності державного органу значною мірою визначається ступенем відповідності державних службовців посадам, котрі вони займають чи мають зайняти. Виявити ступінь відповідності службовців вимогам посади у державному органі можна у процесі нормативно встановленої процедури добору та розстановки кадрів, а саме конкурсної процедури прийому на державну службу. Необхідність та значення конкурсної процедури вступу на державну службу зростають за сучасних