УДК: 094

ГУЗ Анатолій Михайлович

ЕВОЛЮЦІЯ СВІТОВИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Постановка проблеми. 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 – це діяльність, що полягає у встановленні положень для загального і багаторазового застосування щодо наявних чи можливих завдань із 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 виступає продукція, процеси та послуги, зокрема матеріали, приміщення, обладнання, системи, їх сумісність, правила, процедури, форми, методи чи діяльність загалом.

Метою стандартизації у сучасному світі є забезпечення безпеки життя та здоров'я людини, тварин, рослин, а також майна й 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.

Аналіз останніх досліджень і публікацій свідчить, що українські вчені значну увагу приділяють цьому питанню, підтверджуючи беззаперечну його актуальність. Переважна більшість зарубіжних та вітчизняних дослідників висвітлює теоретичні основи стандартів інформаційної безпеки. Натомість еволюція світових стандартів інформаційної безпеки лишається поза увагою науковців. Варто зазначити й про останні фундаментальні праці із цієї проблеми К.Белякова [1], Н.Кушакової-Костицької [2], Л.Задорожньої [3], В.Сідака, В.Артемова [4], О.Богданова, О.Бакалинського [5] та інших.

Метою статті є характеристика еволюції стандартів інформаційної безпеки.

Виклад основного матеріалу. Європейська політика у сфері стандартизації базується на таких принципах: забезпечення участі фізичних і юридичних осіб у розробленні стандартів та вільному виборі видів стандартів при виробництві чи постачанні продукції; відкритість і 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 обов'язкове 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), зі штаб-квартирою в Женеві. Першочерговою її метою було формування системи стандартів, яка б сприяла міжнародній торгівлі. Більшість країн світу має національні представництва та національні комітети в ISO.

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

Міжнародною організацією зі стандартизації прийнято низку стандартів, які діють в 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 рр. XX ст. Передусім вони стосувалися інформаційної безпеки ПЕОМ.

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

"Європейські критерії" (1986 р.) – ґрунтовніший документ, на рівні базового документа у 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, почали розглядати інформаційні технології незалежно від їх призначення, визначаючи розходження тільки в характеристиках середовища їх експлуатації.

"Канадські критерії" (1993 р.) характеризують галузь застосування усіх типів 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 рр. XX ст. – узгодженість позицій та запитів виробників, споживачів й аналітиків щодо класифікаторів продуктів інформаційних технологій.

Як загальні показники, стандарти, які характеризують інформаційну безпеку, фахівці називають такі: універсальність, гнучкість, гарантованість, реалізацію та актуальність.

Найбільш повно критерії для оцінювання механізмів безпеки програмно-технічного рівня представлені у міжнародному стандарті

ISO 15408: Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінювання безпеки інформаційних технологій), прийнятому в 1999 році.

Загальні критерії оцінювання 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 й вимог із фізичного захисту, які безпосередньо пов'язані з описаними функціями безпеки.

Ключовим міжнародним стандартом із безпеки інформації є розроблені 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 у галузі інформаційних технологій [5]. ISO 17799 містить практичні правила з управління інформаційною безпекою і може використовуватися як критерії для оцінювання механізмів безпеки організаційного рівня, включаючи адміністративні, процедурні та фізичні заходи захисту.

Варто зазначити, що цей стандарт бере свій початок із 90-х рр. XX ст. Саме у 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 тощо, зайнявся розробленням стандарту управління інформаційною безпекою; у 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 мала рекомендаційний характер, а друга була призначена для сертифікації та містила частину обов'язкових вимог, що не входили у першу частину.

У 1999 році була опублікована друга частина стандарту: BS 7799, частина 2 "Системи управління інформаційною безпекою – Специфікація та керівництво щодо застосування". На її базі був створений 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. мав помірну популярність лише в країнах британської співдружності.

Наприкінці 1999 р. експерти Міжнародної організації зі стандартизації ISO дійшли висновку, що у межах чинних стандартів ISO відсутній спеціалізований стандарт управління інформаційною безпекою. Було ухвалене рішення не починати розроблення нового стандарту, а, узгодивши із Британським інститутом стандартів, прийняти стандарт ISO 17799 на базі BS 7799:1.

Саме тому у 2000 р. BS 7799:1 став ISO 17799, одержавши статус міжнародного стандарту, що значно змінило ставлення 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 і контроль за ними; політика захисту даних.

У середині 2001 р. були різні погляди на стандартизацію з інформаційної безпеки. Існували різні стандарти, застосування яких на практиці викликало питання та серйозні сумніви. Крім того, більшість фахівців надавала перевагу технологічному підходу до захищеності (тобто визнавала 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].

Із 2003 р. простежується 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 чисельності 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 застосовуватися на практиці (або прийшло усвідомлення необхідності його використання як кращої світової практики).

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

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

У 2005 році вийшла нова редакція стандарту ISO 17799:2005 – сертифікаційний стандарт ISO 27001. У 2007 році ISO 17799 було переопрацьовано й перевидано під номером ISO / IEC 27002.

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

ISO 17799:2007 (ISO/IEC 27002) складається із 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 удосконалити наявні методи інформаційного захисту [6].

Висновки. Дослідивши еволюцію стандартів інформаційної безпеки із 80-х рр. XX ст. до першого десятиліття XXI ст., зазначимо, що стандарти з інформаційної безпеки містять рекомендації з управління інформаційною безпекою, призначені для співробітників, відповідальних за створення, впровадження й підтримку заходів, які забезпечують безпеку на державному підприємстві або в недержавній організації. Рекомендації, наведені в стандартах інформаційної безпеки, використовують з урахуванням національних законів і нормативних вимог. Наразі міжнародні стандарти інформаційної безпеки все більше стають основою для розроблення стандартів безпеки й ефективних методів управління інформаційною безпекою в конкретній організації, на підприємстві, в установі.

Список використаних джерел

1. Беляков К. Інформатизація організаційно-правової сфери суспільної діяльності / К.Беляков // Право України. – 2004. – № 6. – С. 88–92.

2. Кушакова-Костицька Н. Від свободи слова до інформаційного суспільства / Н.Кушакова-Костицька // Право України. – 2004. – № 7. – С. 129–133.

3. Задорожня Л. До питання огляду законодавства в інформаційній сфері / Л.Задорожня // Правова інформатика. – 2004. – № 3. – С. 18–23.

4. Артемов В. Міжнародний стандарт ISO 17799 як складова в галузі менеджменту інформаційної безпеки [Електронний ресурс]. / В.Артемов // Юридичний журнал "ЮСТИНІАН". – 2007. – Режим доступу : http://www.justinian.com.ua/article.php?id=2802.

5. Богданов О. Адаптація міжнародного стандарту управління інформаційною безпекою ISO / IEC 27001:2005 у структурах державного управління України [Електронний ресурс] / О.Богданов, О.Бакалинський. – Режим доступу : http://nc.nusta.com.ua/Kyrsi%202009/tezi/images_tezi/S_6_Bogdanov_ Bakalynsky_1.htm.

6. Анализ международного стандарта ISO 15408 : информационная технология, методы и средства // Бизнес и безопасность. – 2007. – № 561.

Аннотация: В статье охарактеризован процесс становления и развития мировых стандартов информационной безопасности в 80-х гг. XX ст. – нач. XXI ст.

Ключевые слова: стандартизация, информационная безопасность, стандарты информационной безопасности.

Abstract: The article characterizes the process of formation and development of international standards of information security since 80 years of the twentieth century till the first decade of the XXI century.

Key words: standardization, information security, information security standards.