Тема 6. Стандартизація та сертифікація в галузі інформаційної безпеки

Відносини, пов'язані з діяльністю у сфері стандартизації та застосування її результатів, регулюються Законом України «Про стандартизацію» від 17.05.2001. Цей Закон встановлює правові та організаційні засади стандартизації в Україні та спрямований на забезпечення єдиної політики у цій сфері.

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 України 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.

Державна 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 Україні міжнародних та регіональних стандартів;

– дотримання міжнародних та європейських правил і процедур стандартизації;
– участь у Міжнародній (регіональній) стандартизації.

Суб'єктами стандартизації є:

– центральний орган виконавчої влади у сфері стандартизації;
– рада стандартизації;
– інші суб'єкти, що займаються стандартизацією.

Залежно від рівня суб'єкта стандартизації, який приймає чи схвалює стандарти, розрізняють:

– національні стандарти, кодекси усталеної практики та класифікатори, прийняті чи схвалені центральним органом виконавчої влади у сфері стандартизації, видані ним каталоги та реєстри загальнодержавного застосування;
– стандарти, кодекси усталеної практики та технічні умови, прийняті чи схвалені іншими суб'єктами, що займаються стандартизацією.

Застосування стандартів чи їх окремих положень 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.

Міжнародні стандарти та стандарти інших країн

Міжнародні стандарти та стандарти інших країн, якщо їх вимоги не суперечать законодавству України, можуть бути застосовані в Україні в установленому порядку шляхом посилання на них у національних та інших стандартах.

Таким чином виникає питання: що ж таке ISO? Це міжнародна організація зі стандартизації, котра була створена в 1947 р., штаб-квартира в Женеві. Першочерговою її метою було створення лише системи стандартів, яка б сприяла міжнародній торгівлі. Більшість країн світу мають національні представництва та національні комітети в ISO. ISO не працює наодинці. В своїй діяльності вона взаємодіє з іншими міжнародними організаціями зі стандартизації. В галузі інформаційної безпеки такою організацією є для неї МЕК — 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.

Саме з цієї причини правильною та повною назвою нашого стандарту є ISO/IEC 17799 2005 Information Security Management Standard, тобто стандарт ІСО та МЕК з управління інформаційною безпекою.

ISO взаємодіє не лише з міжнародними спеціалізованими організаціями в галузі стандартизації, але й з найбільшими національними. Із цієї причини наш стандарт виник не на порожньому місці: він розроблений на основі британського стандарту BS 7799, що призначений для управління інформаційною безпекою організації незалежно від її сфери діяльності.

Даний стандарт припускає, що служба безпеки, ІТ-відділ (відділ інформаційних технологій), керівництво компанії повинні працювати відповідно до загального регламенту, незалежно від того, мова йде про захист паперового документообігу чи електронних даних.

В останні кілька років ISO 17799 почав упевнено просуватися по країнах СНД. У Республіці Бєларусь з 01.11.2004 р. став національним державним стандартом; у Молдові, завдяки позиції Національного Банку, всі банки з 2003 р. проходять регулярну перевірку на відповідність ISO 17799; у Росії стандарт ISO 17799 перевтілений у держстандарт: прийняття Держстандарту 17799 відбулося в 2006 р.

Сьогодні стандарт ISO 17799 міцно ввійшов у наше життя, ставши на практиці де-факто стандартом побудови систем управління інформаційною безпекою провідних компаній як в Європі та Азії, так і в країнах СНД. До 2005 р. навчальний курс, розроблений підприємством Digital Security, був єдиним у СНД курсом з цього стандарту. Вартість навчання на цих курсах — від 1000 до 2000 дол. США. До теперішнього часу в країнах СНД пройшли навчання кілька тисяч фахівців різних компаній, при цьому курс неодноразово проводився в таких містах як Київ, Дніпропетровськ, Одеса, Кишинів, Рига, Таллінн, Алмати, Ташкент, Москва.

Цікавим було б розглянути (хоча б загалом) історію стандарту ISO 17799.

У середині 90-х років Британський інститут стандартів (BSI) за участі комерційних організацій, таких як Shell, National Westminister Bank, Мішапсі Bank, Umlever, British Telecommunications, Marks & Spencer, Logka та ін., зайнявся розробкою стандарту управління інформаційною безпекою, в 1995 р. був прийнятий національний британський стандарт BS 7799 з управління інформаційною безпекою та її організації незалежно від сфери діяльності. Перша частина стандарту носила рекомендаційний характер, а друга була призначена для сертифікації та містила частину обов’язкових вимог, що не входили в першу частину.

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 за узгодженням із британським інститутом стандартів, взявши за базу BS 7799:1, прийняти стандарт ISO 17799.

Відповідно, 2000 р. вдихнув нове життя в BS 7799:1, ставши ISO 17799, одержав вже статус міжнародного стандарту, що кардинально змінило розміщення сил і відношення до стандарту (між локальним і міжнародним стандартом різниця очевидна).

Що ж стосується офіційної сертифікації по ISO 17799, то вона споконвічно не була передбачена (повна аналогія з BS 7799). Була передбачена тільки сертифікація по BS 7799:2, що являв собою низку обов'язкових вимог (не ввійшли в першу частину BS 7799/ISO 17799). Процедура сертифікації по ISO повинна була з'явитися тільки після виходу в рамках ISO стандарту аналога BS 7799:2 (відзначимо, що це трапилося тільки наприкінці 2005 р. з виходом сертифікаційного стандарту ISO 27001).

Загальна лібералізація ринку інформаційної безпеки призвела до того, що в Білорусії — першій із країн СНД — у листопаді 2004 р. був прийнятий Держстандарт 17799. Аналіз і управління інформаційними ризиками — основа стандарту ISO 17799 — міцно ввійшли в життя більшості фахівців і стали застосовуватися на практиці.

Число компаній у світі, що одержали офіційний сертифікат — більше 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.

Буквально вибуховий інтерес учасників ринку країн СНД до стандарту. Росія, Казахстан, Молдова, Узбекистан, Україна — стандарт став повсюдно

застосовуватися на практиці (або прийшло усвідомлення необхідності його застосування як кращої світової практики).

Порівняльний аналіз стандартів інформаційної безпеки

Головна задача стандартів інформаційної безпеки — узгодженість позицій та запитів виробників, споживачів і аналітиків класифікаторів продуктів інформаційних технологій. Кожна з категорій фахівців оцінює стандарти та вимоги і критерії, які в них існують, за своїми особистими параметрами. Для споживачів найбільшу роль грає простота критеріїв та однозначність параметрів вибору захищеної системи, а для найбільш кваліфікованої частини споживачів — гнучкість вимог та можливість їх застосування до специфічних ІТ- продуктів та середовища експлуатації. Виробники потребують від стандартів максимальної конкретності та спільних вимог і критеріїв з сучасними архітектурами ВР та з розповсюдженими ОС.

Експерти по кваліфікації мріють про стандарти, які детально регламентують процедуру кваліфікаційного аналізу, та про чіткі, прості, однозначні і легкі критерії які споживаються. Очевидно, що подібний ідеал є недосяжним, і реальність його потребує від кожної сторони визначених компромісів. Через це не будемо проводити суб’єктивний аналіз стандартів з точки зору кожного з тих що беруть участь в створенні захищених систем, а спробуємо ввести загальні для всіх “об’єктивні” критерії зіставлення.

У якості загальних показників, стандарти які характеризують інформаційну безпеку і мають значення для трьох груп, можливо назвати універсальність, гнучкість, гарантованість, реалізація та актуальність.

Універсальність стандарту визначається множиною типів ВР та областей їх споживання, до котрих може бути коректно застосовані його положення. Це дуже важлива характеристика стандарту, так як інформаційні технології переживають період бурхливого розвитку, архітектура комп’ютерних систем постійно

удосконалюється, а сфера їх споживання постійно розширюється. Стандарти інформаційної безпеки у своєму розвитку не провині залишатися від інформаційних технологій, що тільки може бути забезпечено гнучкістю вимог і критеріїв які пропонуються.

Під гнучкістю стандарту визначається можливість та зручність його застосування до постійно розвитку інформаційних технологій, а також час, на протязі якого він зберігає свою актуальність. Гнучкість може бути досягнута виключно через фундаментальність вимог та критеріїв і їх інваріантність по відношенню до механізму реалізації та технологіям створення IT- продуктів. Однак очевидно, що надмірна абстрактність вимог і відірваність їх від практики знижує їх реалізацію.

Гарантованість визначає міцність передбачених стандартом методів та засобів затвердження надійності підсумків кваліфікаційного аналізу. Спочатку цьому питанню не приділялося багато уваги, але аналіз опиту споживання перших стандартів інформаційної безпеки показав, що для досягнення передбачених цілей аналітики — класифікатори повинні мати можливість обґрунтувати свої висновки, а розробники потребують механізмів, з допомогою котрих вони могли би підтвердити коректність своїх домагань і представити споживачам визначені гарантії.

Реалізація — це можливість адекватної реалізації вимог і критеріїв стандарту на практиці, з урахуванням витрат на цей процес. Реалізація дуже пов’язана з універсальністю та гнучкістю, але відображає чисто практичні та технологічні аспекти реалізації положень стандарту.

Актуальність відображає відповідальність вимогам та критеріям стандарту множені загроз безпеки які постійно розвиваються та найновішим методам та засобам, які використовуються злочинцями. Ця характеристика, поряд з універсальністю, є одною з найбільш важливих, так як здібність протистояти

загрозам та прогнозувати їх розвиток фактично визначає придатність стандарту і є вирішальним чинником при визначені його придатності.