УДК 004.056:006.057

Концепція актуальності стандартизації в сфері безпеки інформаційних технологій

Поліщук Л.І., старший викладач, pli_80@ukr.net
Кіровоградський національний технічний університет, м. Кіровоград

Досвід світової спільноти показує, що проблема стандартизації в області безпеки інформаційних технологій є об'єктом активних дискусій. На сьогоднішній день можна з впевненістю стверджувати, що в світі відбулася переоцінка підходів до рішення цієї проблеми.

Оскільки ISO (International Organization for Standardization – Міжнародна організація зі стандартизації – існує з 1947 року) тісно працює з міжнародними організаціями і комітетами, а зокрема з Міжнародною електротехнічною комісією IEC (International Electronical Commission – існує з 1906 року), то стандарти ISO/ IEC саме і є міжнародними стандартами для різного роду електричних, електронних, електротехнічних засобів.

Україна, в тому числі, не залишається осторонь від стандартизації сучасних інформаційно-комунікаційних технологій і з 2001 року, вона також активно бере участь в роботі різних комітетів і підкомітетів ISO.

Результатом співпраці під егідою ISO стала розробка широкого спектру стандартів для інформаційної безпеки. Наведемо основні, розроблені комітетами:

1. ISO/IEC 27001:2005 Інформаційні технології. Методи забезпечення безпеки. Системи керування інформаційною безпекою. Вимоги.
2. ISO/IEC 27002:2005 Інформаційні технології. Методи забезпечення безпеки. Практичні правила керування інформаційною безпекою.
3. ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Керування ризиками інформаційної безпеки.
4. ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації систем керування інформаційною безпекою.
5. ISO/IEC 17799:2005 Інформаційні технології. Методи забезпечення безпеки. Практичні правила керування інформаційною безпекою.
6. ISO/IEC TR 18044:2004 Інформаційні технології. Методи забезпечення безпеки. Керування інцидентами інформаційної безпеки.

Ще одним важливим стандартом є так звані Загальні критерії (Common Criteria) — розроблений за участю урядів, визнаний у всьому світі стандарт ISO в галузі оцінювання захищеності IT-продуктів та систем. Загальні критерії передбачають сертифікацію програмних продуктів незалежною акредитованою лабораторією з обов'язковим прискіпливим тестуванням і вивченням документації.

Нажаль, наведені стандарти досі не отримали вітчизняних аналогів, що значно уповільнює процеси стандартизації національних розробок в галузі безпеки інформаційних технологій. Нині стандартизація та щонайменша уніфікація підходів до визначення якості комп'ютерних програм, засобів, систем тощо залишається досить низькою.

В Україні існують законодавчі підстави необхідної сертифікації. Але, вітчизняний сертифікат не є дійсним за межами держави. Для дійсного визнання світовою спільнотою необхідна сертифікація відповідно ISO 9001:2000 у спеціальних інституціях, таких, наприклад, як ABS Quality Evaluations (США), Lloyd's Register Quality Assurance (Великобританія), TUV (Німеччина), Bureau Veritas Quality International (Франція) та ін.

Схвалення подібних інстанцій необхідне компаніям, що пропонують товари чи послуги іноземним клієнтам, у тому числі й засобам безпеки, що прагнуть створити гідну конкуренцію зарубіжним аналогам. Ці та інші протиріччя ускладнюють процес інтеграції нашої держави у світовий інформаційний простір.

Висновки. Наше дослідження не вичерпує всіх аспектів проблеми. Подальшого вивчення потребує іноземний досвід стандартизації засобів захисту і безпеки інформаційних технологій.