Проблеми захисту інформаційних технологій

А.Ю. Ільніцький,
В.В. Шорошев

Міжнародний досвід розвитку стандартів безпеки інформаційних технологій

Стандарти безпеки комп'ютерних систем у провідних західних країнах, починаючи з 1983 р., успішно розвиваються. При цьому прагнення одночасно задовольнити масових користувачів, розробників і експертів комп'ютерних систем призвело до того, що замість простої універсальної шкали безпеки у складі 6-10 класів (американський стандарт TCSEC, 1983 р., європейські критерії ITSEC, 1991 р.) у останньому кращому стандарті CCITSE, 1996 р. використовується вже понад 280 часткових критеріїв безпеки. Такі критерії доступні тільки професіоналу, а не рядовому користувачеві і це їх недолік.

Стандарти безпеки інформаційних технологій в комп'ютерних системах постійно удосконалюються. За 16 років, починаючи з 1983 р., країнами–розробниками цих стандартів (США, Канада, Англія, Франція, Німеччина, Нідерланди) профінансовані і проведені фундаментальні дослідження, на основі яких у діяльність державних, комерційних структур та спецслужб впроваджені новітні інформаційні технології гарантованого рівня безпеки.

Досягнутий кращий досвід провідних західних країн доцільно використовувати в тій мірі, яка буде найбільш забезпечувати наші потреби з питань технічного захисту інформації (ТЗІ), насамперед, згідно з вимогами національних стандартів щодо їх удосконалення, доповнення і більшої деталізації, але без протиріч з ними.

Ільніцький Анатолій Юхимович — начальник лабораторії захисту інформаційних технологій НДІ НАВСУ, полковник міліції.

Шорошев В'ячеслав Вікторович — кандидат технічних наук, провідний науковий співробітник.

Проаналізуємо більш детально під таким кутом міжнародний досвід розвитку і впровадження стандартів безпеки інформаційних технологій.

Проблема безпеки інформаційних технологій у комп'ютерних системах усім відома, актуальна та потребує, по-перше, систематичного оглядово-аналітичного обговорення шляхів вирішення цієї проблеми і, по-друге, безперервного удосконалення критеріїв її оцінки для трьох основних категорій споживачів: масових (рядових) користувачів, розробників (виробників) та експертів кваліфікаційного аналізу захищених комп'ютерних систем.

Аналіз еволюції розвитку міжнародних стандартів і, особливо, масштабів фінансування та кооперації країн-розробників показав, що провідні західні країни з 1983 по 1999 рр. вклали солідні фінансові інвестиції у наукову розробку і реалізацію нової проблеми 20-го сторіччя та міжнародної спільноти – забезпечення безпеки інформаційних технологій у корпоративних комп'ютерних системах, в інформаційній супермагістралі Internet та в кіберпросторі своїх національних регіонів.

Перелік, основні компоненти безпеки і порівняльна оцінка розроблених міжнародних стандартів наведені в таблиці. Порівняльний аналіз недоліків і переваг цих стандартів, а також декларованих у них компонентів безпеки дозволяє зробити такі висновки і рекомендації в плані перейняття кращого досвіду кооперації провідних країн-розробників стандартів безпеки і доповнення та збагачення ними вимог національних нормативно-законодавчих документів з питань ТЗІ.

Основною тенденцією і головною метою розробки, удосконалення та впровадження цих стандартів було прагнення узгодити позиції і одночасно задовольнити запити трьох основних категорій споживачів інформаційних технологій – користувачів, розробників (виробників) та експертів кваліфікаційного аналізу захищених комп'ютерних систем.

Для користувачів головне значення має простота критеріїв безпеки і однозначність декларованих в них вимог для вибору захищених продуктів інформаційних технологій (ІТ-продуктів), а для найбільш кваліфікованих із них — гнучкість вимог і можливість їх застосування до своїх специфічних ІТ-продуктів та середовищ їх експлуатації.

Розробники вимагають від стандартів (критеріїв) максимальної конкретності, однозначності та сумісності декларованих у них вимог і часткових критеріїв (функціональних, технологічних, архітектурних, загальносистемних, експлуатаційних і т.ін.) з сучасними архітектурами і конфігураціями комп'ютерних систем та операційними системами, що в них використовуються.

Для експерта головне значення має детальність регламентуючих процедур кваліфікаційного аналізу, чіткість, простота, однозначність і легкість у використанні декларованих часткових критеріїв безпеки.

Прагнення досягти компромісу і одночасно задовольнити запити користувачів, розробників та експертів неминуче призвело до великого ускладнення критеріїв безпеки. Саме тому замість 6 - 10 класів безпеки (C1, C2, B1, B2, B3, A1 за американським стандартом TCSEC і F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-DI, F-DC, F-DX за європейськими критеріями ITSEC) у стандартах, що були розроблені пізніше, від універсальної шкали безпеки перейшли поступово до все більш зростаючої кількості часткових критеріїв (FCITS, 1993 р. – більше 160, CTCPEC, 1993 – більше 70, CCITSE, 1996 р. – більше 280). Більш того, якщо раніше посилення рівнів безпеки відбувалось монотонно від нижчих класів до вищих, то в останніх і кращих Єдиних критеріях CCITSE структура часткових критеріїв має вигляд не універсальної шкали, а направленого графа і підвищення рівня безпеки і відбувається при руху по його ребрам. Саме тому, на наш погляд, необхідна розробка версії останнього міжнародного стандарту CCITSE для рядових користувачів.

Серед наведених у таблиці міжнародних стандартів особливої уваги з точки зору перейняття кращого досвіду заслуговують європейські критерії ITSEC, канадські критерії CTCPEC та найбільш усього Єдині міжнародні критерії CCITSE. Основні компоненти безпеки та їх суттєвий склад більш детально наведені в умовних позначеннях в таблиці. Безумовно, вони заслуговують на увагу, але в подальшому висновки і рекомендації стосуються останніх Єдиних критеріїв CCITSE, які визнані як міжнародний стандарт ISO.

Порівняльна оцінка міжнародних стандартів інформаційної безпеки

Стандарти безпеки	Ключові компоненти безпеки	Кількість критеріїв (вимог) безпеки	Категорії користувачів стандарту безпеки	Показники якості стандартів безпеки				
				Універ-сальність	Гнучкість	Гаранто-ваність	Реалізує-мість	Акту-альність
Оранжова книга, TCSEC, 1983	ТСВ, ПБ, А3З, К3З	Сім класів безпеки (Д1,С1,С2,В 1,В2, В3,А1)	МО США, К, Р, ЕКА, держструк-тури	Обмежена	Обмежена	Обмежена	Висока (крім класа А1)	Помірна
Європейські критерії ITSEC, 1991	ПБ, АДЗЗ (К3З+Е3З) ЗЗКІ, ЗЗЦІ, ЗЗДІ	Сім рівнів АДЗЗ(Е0-Е6), Десять класів безпеки (F-C1, F-C2,F-B1, FB2, F-B3,F-IN, F-AV,F-DI,F-DC,F-DX)	К, Р, ЕКА	Помірна	Помірна	Помірна	Висока	Помірна
Документи ДТК Росії, 1992	Захист від НСД	Три класи для АС (1-3), Дев'ять класів для ЗОТ (3Б, 3А, 2А, 2Б, 1Д, 1Г,1В, 1Б, 1А)	К, Р, ЕКА	Обмежена	Обмежена	Відсутня	Висока	Обмежена
Федераль-ні критерії FCITS,1992	ІТ-продукт, ПБ, ПФЗ, ТСВ,ФВЗЗ, ВТЗЗ,КАЗЗ	Більше 160 часткових критеріїв	К, Р, ЕКА, ПФЗ-для середи ІТ-продукти	Висока	Відмінна	Достатня	Висока	Висока

Стандарти безпеки	Ключові компоненти безпеки	Кількість критеріїв (вимог) безпеки	Категорії користувачів стандарта безпеки	Показники якості стандартів безпеки				
				Універсальність	Гнучкість	Гарантованість	Реалізуємість	Актуальність
Канадські критерії CTCPEC, 1993	ПБ, ПФЗ, ТСВ, теги (tag), ЗЗКІ, ЗЗЦІ, ЗЗПС, ЗЗАС, АДЗЗ	Вісім рівнів АДЗЗ (Т0-Т7), більше 70 часткових критеріїв безпеки	П, Р, ЭКА	Помірна	Достатня	Достатня	Достатня	Середня
Єдині критерії CCITSE, 1996 Загальна методологія оцінки безпеки інформ. технологій, 1997	ПБ,ПФЗ, ПТЗ,ТСВ, ІТ-продукт, ЗЗКІ,ЗЗЦІ, ЗЗПС,ЗЗАС	Більше 280 часткових критеріїв безпеки	К, Р,ЕКА, ПФЗ-для користувачів ІТ-продукту	Надмірна	Надмірна	Надмірна	Надмірна	Надмірна

Умовні позначення: ПБ – політика безпеки, КЗЗ – коректність засобів захисту, АЗЗ – аудит засобів захисту, ТСВ – надійна обчислювальна база (trsted computer base), АДЗЗ – адекватність засобів захисту, К – користувачі, Р – разробники засобів захисту, ЕКА – експерти кваліфікаційного аналізу, ПФЗ – профіль захисту, ПТЗ – проект захисту, ЕЗ – ефективність засобів захисту, ЗЗКІ – захист від загроз конфіденційності інформації, ЗЗЦІ – захист від загроз цілістності інформації, ЗЗАС – захист від загроз аудиту системи, ЗЗПС – захист від загроз працездатності системи, ЗЗДІ – захист від загроз доступності інформації, АС – автоматизована система, ФВЗЗ – функциональні вимоги до засобів захисту, ТРЗЗ – вимоги до технології розробки засобів захисту, КАЗЗ – вимоги до кваліфікаційного аналізу засобів захисту.

Основними концептуальними компонентами безпеки інформаційних технологій згідно з Єдиними міжнародними критеріями CCITSE є потенційні загрози безпеки і типові задачі захисту під них, політика безпеки, IT-продукт, профіль захисту, проект захисту, функціональні вимоги до засобів захисту та адекватності засобів захисту.

Основними потенційними загрозами для безпеки інформації та відповідно типовими концептуальними задачами захисту від НСД в Єдиних міжнародних критеріях CCITSE є такі:

захист від загроз конфіденційності (несанкціонованого одержання) інформації по всім каналам її витоку (офіційно легалізуються потайні канали зв'язку, але відсутні канали витоку по ПЕМВН, що є їх недоліком);

захист від загроз цілісності (несанкціонованої зміни) інформації;

захист від загроз доступності інформації (несанкціонованого або випадкового обмеження) інформації та ресурсів самої системи;

захист від загроз аудиту системи (декларовано 12 потенційних загроз, наприклад, загрози від несанкціонованих атак або вторгненнь у систему, маніпуляцій з протоколами обміну та аудіту, з загальносистемним програмним забезпеченням і т.ін.).

Під політикою безпеки декларується набір законів, норм і правил, регламентуючих порядок обробки, захисту та поширення інформації комп'ютерної системи даної організації. Наше поняття "концепції ТЗІ" більш повне та доцільне, тому що, по-перше, включає в себе більше компонентів безпеки, а по-друге, містить у собі основні концептальні положення щодо порядку їх практичної реалізації і забезпечення, наприклад, включно до навчання і перепідготовки кадрів фахівців з питань ТЗІ, системи керівництва і контролю комплексної системи ТЗІ і т. ін..

Під IT-продуктом декларується сукупність апаратних і\або програмних засобів, що постачається кінцевому споживачеві як готовий до використання засіб обробки інформації. Сукупність IT-продуктів об"єднується в функціонально-закінчений комплекс (продукт) для рішення конкретної прикладної задачі в системі обробки інформації.

Принциповою різницею між ІТ-продуктом (для нас незвичний, але досить доцільний термін) **і системою обробки інформації** є те, що ІТ-продукт звичайно розроблюється для використання в багатьох системах обробки інформації, тому його розробник орієнтується тільки на найбільш загальні вимоги щодо середовища його експлуатації (умови використання і потенційні загрози безпеці інформації). Навпаки, система обробки інформації розроблюється вузькоспеціалізовано для вирішення конкретних прикладних задач та під конткретні вимоги споживачів, що дозволяє у повній мірі враховувати специфіку впливів конкретного середовища експлуатації. Саме тому ІТ-продукт, а не система обробки інформації декларується в CCITSE як універсальна компонента безпеки, а в США, Канаді навіть існують державні каталоги ІТ-продуктів.

Профіль захисту – спеціальний нормативний документ, що регламентує сукупність задач захисту, функціональні вимоги щодо засобів захисту, адекватності засобів захисту та їх обгрунтування. Цінність цієї стандартизованої універсальної компоненти безпеки полягає в тому, що вона визначає вимоги безпеки до відповідної категорії ІТ-продуктів, не уточнюючи методи і засоби їх реалізації. Таким чином, за допомогою профілей захисту споживачі можуть формулювати свої вимоги до розробників ІТ-продуктів. Окремі положення профілю захисту покладено в основу "плану захисту" стандартів ТЗІ України. Суто практично для перейняття кращого міжнародного досвіду проаналізуємо зміст розділів профілю захисту[1].

Введення – містить усю інформацію для пошуку профілю захисту в бібліотеці (каталозі) профілів. Таким чином, для нас було б доцільно ввести "банк ІТ-продуктів з питань ТЗІ";

ідентифікатор профілю захисту – це унікальне ім'я для його пошуку серед подібних йому профілів і позначення посилань на нього;

огляд змісту – коротка анотація профілю захисту, на підставі якої споживач може зробити висновок щодо придатності даного профілю захисту.

Опис ІТ-продукту – коротка характеристика, призначення, принципи роботи, методи використання і т.ін. Ця інформація не підлягає аналізу і сертифікації, але надається розробником

і експертам для тлумачення вимог безпеки та визначення їх відповідності задачам, що вирішуються за допомогою ІТ-продукту.

Середовище експлуатації – опис усіх аспектів функціонування ІТ-продукту, пов'язаних з безпекою;

загрози безпеки – опис потенційних загроз безпеки, які властиві середовищу експлуатації ІТ-родуктів, та яким повинен протистояти захист; для кожної потенційної загрози повинно бути вказано її джерело, а також метод впливу та її об'єкт;

політика безпеки – опис регламентування та пояснення правил політики безпеки, яка повинна бути реалізована в ІТ-продукті;

умови експлуатації – опис умов експлуатації ІТ-продукту з повною характеристикою середовища його експлуатації з точки зору безпеки.

Задачі захисту – потреби користувачів щодо протидій вказаним потенційним загрозам безпеки і\або в реалізації політики безпеки:

задачі захисту ІТ-продукту – визначають та регламентують потреби в протидії потенційним загрозам безпеки і\або в реалізації політики безпеки;

інші задачі захисту – регламентують потреби в протидії потенційним загрозам безпеки і/або в реалізації політики безпеки інших компонентів комп'ютерної системи, що не відносяться до ІТ-технологій (телекомунікаційна безпека, роумінг безпеки при виході на зовнішні мережі, наприклад, Internet, Relcom, Interpol і т.ін..

Вимоги безпеки – вимоги, яким повинен задовольняти ІТ-продукт для вирішення задач захисту (типових, спеціальних і т.ін.):

функціональні вимоги – типові вимоги згідно з критеріями CCITSE, деталізація яких дозволятиме продемонструвати її відповідність задачам захисту;

вимоги адекватності – типові вимоги адекватності згідно з критеріями CCITSE (сім класів і двадцять п'ять вимог та сім рівнів адекватності);

вимоги до середовища експлуатації – необов'язкові і можуть містити вимоги до середовища експлуатації ІТ-продуктів (функціональні, адекватності), при цьому, на відмі-

ну від попередніх розділів, використання типових вимог критеріїв CCITSE є бажаним, але не обов'язковим.

Додаткові відомості – необов'язковий розділ з будь-якою додатковою інформацією, яка корисна для проектування, розробки, кваліфікаційного аналізу і сертифікації ІТ-продукту.

Обгрунтування – необхідно показати, що профіль захисту містить повну і пов'язану множину вимог і що задовольняючий їм ІТ-продукт буде протистояти загрозам безпеки середовища експлуатації:

обгрунтування задач захисту – слід показати, що задачі, які запропоновані в профілі, відповідають властивостям середовища експлуатації, тому що їх вирішення дозволить ефективно протистояти загрозам безпеки та реалізувати політику безпеки;

обгрунтування вимог безпеки – показує, що вимоги безпеки дозволяють вирішити типові задачі захисту, оскільки:

а) сукупність цілей по функціональним вимогам відповідає визначеним задачам захисту;

б) вимоги безпеки є узгодженими, тобто не протирічать, а навпаки підсилюються;

в) усі взаємозв'язки між вимогами (функціональними, адекватності, до середовища експлуатації) враховані або шляхом вказівки їх в вимогах, або шляхом декларування вимог до середовища експлуатації;

г) обраний набір вимог і рівень адекватності (один з семи стандартизованих рівнів по CCITSE) можуть бути обгрунтовані та гарантовані.

Профіль захисту є порадником для розробника і виробника ІТ-продукту, які на його підставі та запропонованих їм рекомендацій повинні розробити так званий "проект захисту", що є порадником для кваліфікаційного аналізу і сертифікації ІТ-продукту.

Проект захисту – новий нормативний документ, введений уперше в критеріях CCITSE, регламентує типові задачі захисту, функціональні вимоги та вимоги адекватності до засобів захисту, їх загальну специфікацію, а також їх обгрунтування. Багато розділів співпадають з профілем захисту, але це самостійний документ, який є порадником для експертів кваліфікаційного аналізу

та сертифікації ІТ-продуктів, тому доцільно проаналізувати його зміст[2]:

введення – інформація, що необхідна для ідентифікації проекту захисту, визначення його цільового призначення та огляду його змісту;

ідентифікатор – унікальне ім'я проекту захисту для його пошуку та ідентифікації, а також відповідного йому ІТ-продукту;

огляд змісту – досить детальна анотація проекту захисту, що дозволяє споживачам визначити придатність ІТ-продукту для рішення задач;

заявка на відповідність вимогам CCITSE – повинна містити опис усіх властивостей ІТ-продукту, які підлягають кваліфікаційному аналізу по CCITSE.

Опис ІТ-продукту – аналогічно профілю захисту.

Середовище експлуатації – аналогічно профілю захисту.

Задачі захисту – аналогічно профілю захисту.

Вимоги щодо безпеки проекту захисту – містять вимоги до ІТ-продукту, яких додержувався виробник при його розробці, що дозволяє йому заявити про успішне рішення поставлених задач захисту:

функціональні вимоги до ІТ-продукту на відміну від аналогічних у профілі захисту допускають використання, окрім типових вимог CCITSE, інших специфічних вимог для даного продукту та середовища його експлуатації, але у форматі вимог CCITSE;

вимоги адекватності – аналогічні по змісту, як у профілі захисту, але можуть включати рівні адекватності, які не декларовані в CCITSE. У цьому випадку опис рівня адекватності повинен бути чітким, непротирічним та мати ступінь деталізації, що допускає його використання у ході кваліфікаційного аналізу, але обов'язково у форматі вимог CCITSE.

Загальна специфікація ІТ-продукту – визначає реалізацію ІТ-продуктом вимог безпеки за допомогою визначення високорівневих специфікацій функцій захисту, що реалізують функціональні вимоги та вимоги адекватності CCITSE;

специфікації функцій захисту – описують функціональні можливості засобів захисту ІТ-продукту, які заявлені його розробником як такі, що реалізують декларовані вимоги безпеки. Фор-

ма представлення специфікацій повинна дозволяти визначити відповідність між функціями захисту та вимогам безпеки;

специфікації рівня адекватності – визначають заявлений рівень адекватності захисту ІТ-продукту та його відповідність вимогам адекватності у вигляді надання параметрів технологій проектування та створення ІТ-продукту; ці параметри повинні бути представлені у форматі, що дозволяє визначити їх відповідність стандартним вимогам адекватності по CCITSE.

Заявка на відповідність профілю захисту – проект захисту повинен задовольняти вимогам одного або декількох профілів захисту. Цей необов'язковий розділ має містити матеріали, що необхідні для підтвердження заявки. Для кожного профілю захисту цей розділ повинен містити таку інформацію:

посилання на профіль захисту – одночасно ідентифікує профіль захисту, на реалізацію якого претендує проект безпеки з вказівкою випадків, у яких рівень захисту, що забезпечується, перевищує вимоги профілю з коректною реалізацією включно до всіх його вимог;

відповідність профілю захисту – визначає можливості ІТ-продукту, які реалізують задачі захисту та вимог, що містяться в профілі захисту;

удосконалення профілю захисту – відображають можливості ІТ-продукту, які виходять за рамки задач захисту та вимог, які встановлені в профілі захисту.

Обгрунтування – повинно показати, що проект захисту містить повну та зв'язану множину вимог, що реалізуючий його ІТ-продукт буде ефективно протидіяти загрозам безпеки середовища експлуатації та що загальні специфікації функцій захисту відповідають вимогам безпеки. Крім того, обгрунтування містить підтвердження заявленої відповідності профілю захисту. Розділ деталізується в такому:

обгрунтування завдань захисту – повинно показати, що задачі захисту, заявлені в проекті захисту, відповідають властивостям середовища експлуатації, тобто їх вирішення дозволить ефективно протидіяти загрозам безпеки та реалізовувати обрану під них політику безпеки;

обгрунтування вимог безпеки – показує, що вимоги безпеки дозволяють вирішити завдання захисту, оскільки:

а) функціональні вимоги безпеки відповідають задачам захисту;

б) вимоги адекватності відповідають функціональним вимогам та підсилюють їх;

в) набір усіх функціональних вимог (стандартних по CCITSE та специфічних) забезпечує рішення задач захисту;

г) усі взаємозв'язки між вимогами CCITSE враховані або шляхом їх вказівки в самих вимогах, або шляхом пред'явлення відповідних вимог до середовища експлуатації;

д) усі вимоги безпеки успішно реалізовані;

е) заявлений рівень адекватності може бути підтверджений;

обгрунтування функцій захисту – має демонструвати їх відповідність функціональним потребам безпеки та задачам захисту. Для цього має бути обгрунтовано, що:

а) вказані функції захисту відповідають заявленим задачам захисту;

б) сукупність вказаних функцій захисту забезпечує ефективне рішення сукупності задач захисту;

в) заявлені можливості функцій захисту відповідають дійсності;

обгрунтування рівня адекватності – підтверджує, що заявлений рівень безпеки відповідає вимогам адекватності.

обгрунтування відповідності профілю захисту – демонструє, що вимоги проекту захисту реалізують усі вимоги профілю захисту. Для цього має бути показано, що:

а) усі удосконалення задач захисту в порівнянні з профілем захисту реалізовані коректно та в напряму їх розвитку та конкретизації;

б) усі удосконалення вимог безпеки в порівнянні з профілем захисту реалізовані коректно та в напряму їх розвитку та конкретизації;

в) усі задачі захисту профілю захисту успішно реалізовані та всі вимоги профілю захисту задовільнені;

г) ніякі додатково введені в проект захисту спеціальні задачі захисту та вимоги безпеки не протирічать профілю захисту.

Функціональні вимоги до засобів захисту – в Єдиних критеріях CCITSE декларуються у вигляді добре опрацьованої формальної структури. Набір функціональних вимог узагальнює

усі існуючі раніш стандарти інформаційної безпеки та характеризуються своєю повнотою і детальністю. Вони розбиті на дев'ять класів та 76 розділів функціональних вимог. Кожен розділ має своє унікальне ім'я та шестисимвольний ідентифікатор, який складається з трьохсимвольного позначення розділу. Використовується для здійснення посилань на розділ. Ранжирування функціональних вимог здійснюється не по єдиній універсальній шкалі безпеки, як в критеріях TCSEC, ITSEC, а по множині часткових критеріїв (більш 280). Набір цих критеріїв являє собою ієрархічну структуру у вигляді неупорядкованого списку порівняних та непорівняних вимог, в якому посилення вимог безпеки відбувається монотонно від більш низьких рівнів до більш вищих. Ця структура має вигляд направленого графу. Посилення вимог щодо безпеки відбувається при русі по його ребрам.

Вимоги адекватності засобів захисту – як і функціональні, вимоги адекватності тісно структуровані, в них регламентовані усі етапи проектування, створення та експлуатації ІТпродукту. Структура вимог адекватності аналогічна функціональним вимогам. Ранжирування стандартних вимог представлена у вигляді упорядкованих списків. Критерії адекватності використовуються в ході кваліфікаційного аналізу ІТ-продукту відповідного рівня адекватності.

Рівні адекватності засобів захисту – Єдині критерії CCITSE пропонують сім стандартизованих рівнів адекватності, кожен з яких визначає ступінь відповідності ІТ-продукту кожній вимозі адекватності (адекватність підвищується з першого рівня до сьомого). Назви рівнів відображають можливості засобів контролю та верифікації, які використовуються в ході розробки та аналізу ІТ-продукту (таблиця, крайня права колонка).

Таким чином, Єдині критерії CCITSE концептуально розроблялись у розрахунку на три групи спеціалістів: виробників та розробників, рядових користувачів ІТ-продуктів, а також експертів кваліфікаційного аналізу захищених комп'ютерних систем.

Користувачі можуть розглядати декларування рівнів безпеки ІТ-продукту як метод визначення відповідності ІТ-продукту своїм запитам. Ці запити створюють на підставі результатів проведення аналізу ризиків та вибраної політики безпеки. Єдині критерії CCITSE відіграють суттєву роль у процесі формування запитів ко-

ристувачів, тому що містять механізми, які дозволяють формувати ці запити у вигляді набору стандартизованих вимог (функціональності та адекватності). Це дозволяє користувачам прийняти обгрунтоване рішення про варіантність використання тих чи інших ІТ-продуктів. В решті-решт, Єдині критерії ССІТSЕ надають користувачам механізм профілів та проектів Захисту, за допомогою яких вони можуть формулювати специфічні для них вимоги, не турбуючись про механізми їх реалізації.

Виробники (розробники) можуть використовувати рекомендації Єдиних критеріїв ССІТSЕ в ході проектування, розробки ІТ-продуктів, а також при підготовці до кваліфікаційного аналізу та сертифікації. Рекомендації ССІТSЕ дають можливість виробникам (розробникам) на підставі запитів користувачів визначити низку вимог, яким повинен задовольняти розроблюємий ними ІТ-продукт. Єдині критерії ССІТSЕ пропонують виробникам спеціальний механізм "проекту захисту". Він доповнює "профіль захисту" та дозволяє з'єднати опис механізмів реалізації засобів захисту та вимог, на які орієнтувався розробник.

Експерти кваліфікаційного аналізу можуть використовувати рекомендації ССІТSЕ як критерії для визначення відповідності між ІТ-продуктом та вимогами, що до нього ставляться. Стандарт ССІТSЕ описує тільки загальну схему проведення кваліфікаційного аналізу та сертифікації, але не регламентує процедуру їх здійснення. Питанням методології кваліфікаційного аналізу та сертифікації присвячений окремий документ тих самих авторів ССІТSЕ – "Загальна методологія оцінки безпеки інформаційних технологій", який як доповнення до стандарту ССІТSЕ опубліковано у 1997 р. Набір класів функціональних вимог ССІТSЕ відрізняється від інших стандартів безпеки, по-перше, своєю загальною повнотою (9 класів і 76 розділів вимог) та, по-друге, багаторівневим підходом до забезпечення безпеки. Вперше окремі класи вимог по ССІТSЕ направлені на забезпечення безпеки самих засобів захисту, контроль за експлуатацією системи, забезпечення конфіденційності сеансів доступу до системи та до організації обміну інформацією. Єдині критерії ССІТSЕ декларують сім стандартних рівнів адекватності, які відображають можливості засобів контролю та верифікації у ході розробки, кваліфікаційного аналізу та сертифікації ІТ-продуктів.

Єдині критерії CCITSE розглядають інформаційну безпеку як сукупність типових (концептуальних) задач захисту від загроз конфіденційності (несанкціонованого одержання), цілісності (несанкційної зміни), доступності (несанкціонованого обмеження) та аудиту (несанкціонованого обмеження, підміни контролю) інформації, що захищається, а також ресурсів самої комп'ютерної системи.

Стандарт CCITSE затверджений Міжнародною організацією по стандартизації (ISO) у межах початого цією організацією у 1990 р. проекту по створенню міжнародного стандарту інформаційної безпеки. В межах політики інтеграції, яку проводить Україна щодо європейської спільноти, рекомендації CCITSE представляють безсумнівний інтерес. Оскільки вони мають дуже універсальний і високопрофесійний характер, багато їх рекомендацій та компонентів доцільно використовувати для удосконалення та підвищення безпеки інформаційних технологій в автоматизованих системах ОВС України, що сприятиме їх утвердженню серед спільноти західних спецслужб як провідних в новітніх інформаційних технологіях гарантованої безпеки.

---

[1] Див.: *Зегжда Д.П., Ивашко А.М.*. Как построить защищенную информационную систему. – Санкт-Петербург: НПО "Мир и семья-95", 1997.

[2] Див.: *ДСТУ* 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. – Введ. 01.01.97 р.