УДК 004.056

ОЦІНОЧНІ СТАНДАРТИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Цвілій О.О., Некраш І.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: o.tsviliy@ukr.net

APPRECIATE STANDARDS IN SCOPE OF INFORMATION SECURITY

The comparison of the results of independent security assessments in accordance with the appreciate standards in the scope of information security is considered. The application of criteria for assessing the safety of IT products in Ukraine is explored.

Розглядається забезпечення зіставлення результатів незалежних оцінок безпеки у відповідності до оціночних стандартів у сфері інформаційної безпеки. Досліджується застосування критеріїв оцінки безпеки продуктів ІТ в Україні.

Зіставлення результатів незалежних оцінок безпеки досягається наданням єдиного набору вимог до функціональних можливостей безпеки продуктів ІТ і до заходів довіри, що застосовуються до цих продуктів ІТ при оцінці безпеки. Дані продукти ІТ можуть бути реалізовані у вигляді апаратного, програмно-апаратного або програмного забезпечення.

В процесі оцінки досягається певний рівень впевненості у тому, що функціональні можливості безпеки таких продуктів ІТ, а також заходи довіри, вжиті по відношенню до таких продуктів ІТ, відповідають вимогам, що пред'являються. Результати оцінки можуть допомогти споживачам вирішити, чи відповідають продукти ІТ їхнім потребам в безпеці.

На сьогоднішні день у приватному та банківському секторах використовується міжнародний стандарт ISO/IEC 15408 в трьох його частинах, нова редакція яких знаходиться в стадії розробки [1].

Цей міжнародний стандарт розробляє Об'єднаний технічний комітет ISO/IEC JTC 1, підкомітет SC 27 «IT Security techniques».

Стандарт ISO/IEC 15408-1:2009 «Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model» встановлює загальні концепції та принципи оцінки безпеки інформаційних технологій та визначає загальну модель їх оцінки безпеки, надану різними частинами стандарту ISO/IEC 15408 [2].

Він надає огляд усіх частин стандарту ISO/IEC 15408, визначає терміни й скорочення, встановлює основну концепцію цільової оцінки та контекст оцінки, а також і описує аудиторію, до якої відносяться ці критерії оцінки. Дається вступ до основних концепцій безпеки, необхідних для оцінки ІТ-продуктів.

Інформація, що міститься в системах або продуктах ІТ, є критичним ресурсом, що дозволяє організаціям успішно вирішувати свої завдання. Крім того, приватні

особи вправі очікувати, що їх персональна інформація, розташована в продуктах або системах ІТ, залишається приватною, доступною їм за мірою необхідності і не буде піддаватися несанкціонованій модифікації. При виконанні продуктами або системами ІТ своїх функцій слід здійснювати належне управління інформацією для забезпечення її захисту від небезпек небажаного або необґрунтованого розповсюдження, зміни або втрати. Термін «безпека ІТ» використовується для того, щоб розглянути запобігання та зменшення цих та подібних небезпек.

Багато споживачів ІТ з-за недоліку знань, компетентності чи ресурсів, не впевнені в безпеці застосовуваних продуктів та систем ІТ, можливо, не захочуть покладатися виключно на запевнення розробників. Щоб підвищити свою впевненість у заходах безпеки продуктів або систем ІТ, користувачі можуть замовити аналіз безпеки цього продукту або системи (тобто оцінку безпеки).

У стандарті ISO/IEC 15408-1 представлені очікувані результати оцінки профілів захисту (ПЗ) та оцінки об'єктів (ОО). Оцінки ПЗ або ОО дозволяють створювати каталоги ПЗ або ОО, що пройшли оцінку. Оцінка завдань по безпеці (ЗБ) дає проміжні результати, які потім використовуються при оцінці ОО.

Необхідно, щоб оцінка ПЗ та ОО приводила до об'єктивних і повторюваних результатів, на які можна потім посилатися як на свідчення навіть при відсутності об'єктивної шкали для представлення результатів оцінки безпеки ІТ. Наявність сукупності критеріїв оцінки є необхідною попередньою умовою для того, щоб оцінка призводила до значного результату, надаючи технічну базу для взаємного визнання результатів оцінки різними органами з оцінки відповідності.

Наразі, може стати питання щодо створення таких органів з оцінки відповідності, акредитованих у Національному агентстві з акредитації України.

Практичне застосування критеріїв включає в себе як об'єктивні, так і суб'єктивні елементи оцінки, тому отримання абсолютно точних та універсальних рейтингів безпеки ІТ не представляється можливим.

Рейтинг, отриманий згідно ISO/IEC 15408, представляє підсумкові дані специфічного типу дослідження характеристик безпеки ОО. Такий рейтинг не гарантує придатності до використання у будь-якому конкретному середовищі застосування. Рішення про прийом ОО до використання у конкретному середовищі застосування базується на обліку багатьох аспектів безпеки, включаючи також висновки оцінки.

Зміст та подання функціональних компонентів безпеки в комп'ютерній системі, які повинні бути оцінені визначає стандарт ISO/IEC 15408-2:2008 «Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components» [2]. Він містить повний каталог заздалегідь визначених функціональних компонентів безпеки, які організовані за допомогою ієрархічної структури класів, сімей та компонентів.

Стандарт ISO/IEC 15408-2 також дає вказівки щодо специфікації індивідуальних вимог безпеки, якщо немає відповідних заздалегідь визначених функціональних компонентів безпеки.

Вимоги до забезпечення критеріїв довіри до безпеки в комп'ютерній системі

визначає ISO/IEC 15408-3:2008 «Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components» [2], який визначає зміст та подання вимог довіри до безпеки у формі класів, сімей та компонентів, які представлені в ієрархічному порядку в сімействах, а також містить рекомендації щодо організації нових вимог щодо довіри.

Загальна інформація про методологію оцінки та схема оцінки представлена в стандарті ISO/IEC 18045:2008 «Information technology - Security techniques - Methodology for IT security evaluation», нова редакція якого також знаходиться в стадії розробки [2].

На відміну від ISO/IEC 15408, де кожен елемент у всіх компонентах одного сімейства довіри має один і той же номер, вказаний останньою цифрою його умовного позначення, стандарт ISO/IEC 18045 може вводити нові кроки оцінювання при зміні елемента дій оцінювача з ISO/IEC 15408 в залежності від підвиду діяльності; в результаті остання цифра умовного позначення наступних кроків оцінювання зміниться, хоча крок оцінювання залишиться тим же самим.

Крім того, стандарт ISO/IEC 18045:

а) описує загальні завдання оцінки без визначення вердиктів, пов'язаних з ними, оскільки ці завдання не відображаються на елементи дій оцінювача з ISO/IEC 15408;

б) описує роботи, необхідні для отримання результату оцінки профілю захисту;

в) визначає дії по оцінці, згруповані за класами довіри, та охоплює базові методи оцінки, які використовуються для надання технічних свідоцтв результатів оцінки;

г) наводить пояснення критеріїв оцінки вразливостей і приклади їх застосування.

Варто зазначити, що розширення сфери застосування ISO/IEC 15408 з урахуванням ряду критичних аспектів операційних систем, які не розглядаються в оцінці ISO/IEC 15408, передбачено в стандарті ISO/IEC TR 19791:2010 «Information technology - Security techniques - Security assessment of operational systems», який містить керівництво та критерії оцінки безпеки операційних систем [2]. Основні розширення, що вимагають адресної оцінки операційного середовища, пов’язані з цілями оцінки та декомпозиції складних операційних систем у сфері безпеки, які можуть бути окремо оцінені.

Стандарт ISO/IEC TR 19791 передбачає:

а) визначення та модель для операційних систем;

б) опис розширень до концепцій оцінки ISO/IEC 15408, необхідних для оцінки таких операційних систем;

в) методологію та процес здійснення оцінки безпеки операційних систем;

г) додаткові критерії оцінки безпеки для вирішення тих аспектів операційних систем, які не охоплені критеріями оцінки ISO/IEC 15408.

Цей стандарт дозволяє включити продукти безпеки, що оцінюються відповідно до ISO/IEC 15408, до операційних систем, які оцінюються в цілому за допомогою ISO/IEC TR 19791.

ISO/IEC TR 19791 обмежується оцінкою безпеки операційних систем та не

враховує інші форми оцінки системи, а також не визначає методи ідентифікації, оцінки та прийняття операційного ризику.

Методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів в Україні визначає НД ТЗІ 1.1-002-99.

Спільним наказом Мінюсту та Адміністрації Держспецзв'язку було затверджено Перелік стандартів у сфері електронного цифрового підпису, перспективних для перегляду та гармонізації з європейськими та міжнародними стандартами відповідно до встановлених законодавством процедур, а також, затверджено Перелік національних стандартів у сфері електронного цифрового підпису, що підлягають перегляду. А 25.12.2014 до цього наказу були внесені зміни (№ 2170/5/703) та актуалізовано як Перелік міжнародних та європейських стандартів, інших актів технічного регулювання для гармонізації з метою реформування, розвитку та забезпечення інтероперабельності системи електронного цифрового підпису, де розділ XI «Методи та механізми захисту від несанкціонованого доступу» передбачає в т.ч. стандарти ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 18045 [1].

У 2015 році наказом від 18.12.2015 № 193 було затверджено та прийнято ДСТУ ISO/IEC 18045:2015 Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT (ISO/IEC 18045:2008, IDT).

Вперше в Україні наказом від 04.08.2017 № 207 [3] було затверджено та прийнято ДСТУ ISO/IEC 15408-1:2017 «Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT)», ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (ISO/IEC 15408-2:2008, IDT), ДСТУ ISO/IEC 15408-3:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 3. Вимоги до гарантії безпеки (ISO/IEC 15408-3:2008, IDT), що є дуже важливим кроком для фахівців в області інформаційної безпеки, які сьогодні не можуть обійтися без знань відповідних стандартів.

Література

1. Цвілій О.О., Майстренко А.В. Застосування в Україні критеріїв оцінки безпеки в комп'ютерній системі. - Матеріали 7-ї Міжнародної науково-практичної конференції "ІНФОКОМУНІКАЦІЇ - СУЧАСНІСТЬ ТА МАЙБУТНЄ". 2017. Збірник тез. ст. 131-133.
2. International Organization for Standardization [Електронний ресурс]// – Режим доступу: http://www.iso.org/iso/home.html.
3. Наказ ДП "УкрНДНЦ" від 04 серпня 2017 № 207 «Про прийняття національних нормативних документів, гармонізованих з європейськими нормативними документами, поправки до національного нормативного документа, скасування національних нормативних документів»