УДК 621.39

ОЦІНКА ВІДПОВІДНОСТІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ОСНОВІ ЗІСТАВЛЕННЯ ВИМОГ МІЖНАРОДНИХ СТАНДАРТІВ ТА НАЦІОНАЛЬНИХ НОРМАТИВНИХ ДОКУМЕНТІВ

Горицький В.М., Романченко В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: kiprida3711@gmail.com

Conformity assessment of security of information technology based on a comparison with international standards and national regulations

Generalization of requirements for procedure of qualification analysis regarding information security. Comparison of information security and trust components defined by ISO/IEC 15408 to requirements of ND TZI 2.5-004-99.

Доступ користувачів до інформації, яка є власністю держави, або до інформації з обмеженим доступом слід обробляти в системі із застосуванням комплексних систем захисту інформації(КСЗІ), підтвердження відповідності якої здійснено за результатами державної експертизи. Критерії оцінювання комп'ютерних систем в Україні визначено в НД ТЗІ 2.5-004-99. Разом з тим, на міжнародному рівні використовуються критерії, визначені в стандарті ISO/IEC 15408. Також, діюча в Україні та визнана в світі система оцінки відповідності, включаючи акредитовані органи з оцінки відповідності (ООВ), національну систему акредитації ООВ та їх нотифікацію (за потреби), також передбачає використання тільки відповідних міжнародних стандартів.

Ціль дослідження: створення єдиної системи критеріїв та оцінки відповідності безпеки інформаційних технологій шляхом їх гармонізації з міжнародними стандартами. В роботі представлені приклади гармонізованого стандарту.

Кваліфікаційний аналіз засобів захисту інформації проводять з метою оцінювання відповідності фактичної реалізації певним вимогам: вимогам нормативних документів у сфері технічного захисту інформації (ТЗІ), технічного завдання та іншої документації.

Українська нормативна база передбачає такі види кваліфікаційного аналізу: атестація (комплексів ТЗІ); державна експертиза (КСЗІ, засобів ТЗІ); сертифікація (зокрема засобів, ТЗІ).

Міжнародна нормативна база оперує поняттями: критерії, оцінка відповідності, акредитовані органи з оцінки відповідності, акредитація ООВ тощо.

Акредитація органів з оцінки відповідності – засвідчення органу з оцінки відповідності вимогам національних стандартів, гармонізованих з відповідними міжнародними та європейськими стандартами.

Мета державної експертизи - оцінка захищеності інформації, яка обробляється або циркулює в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [1].

Порядок проведення експертизи визначено у Положенні про державну експертизу у сфері технічного захисту інформації. На основі результатів державної експертизи підтверджують відповідність КСЗІ та надають Атестат відповідності [1].

Сертифікацію засобів забезпечення ТЗІ здійснюють із метою підтвердження їх відповідності вимогам нормативних документів.

Таблиця 1. Відомості щодо зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99.

Вимоги НД ТЗІ 2.5-004-99 щодо політики функціональних послуг безпеки	**Вимоги стандарту ISO/IEC 15408-2 щодо функціональних елементів функціональних компонентів безпеки, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення функціональними елементами вимог НД ТЗІ 2.5-004-99**
Політика довірчої конфіденційності, що реалізується комплекс засобів захисту (КЗЗ), повинна визначати множину об'єктів експертизи (ОЕ), до яких вона відноситься	Функції безпеки об’єкта (ФБО) повинні реалізовувати політику функцій безпеки (ПФБ) керування доступом для списоку суб’єктів, на які поширюється ПФБ.	У списку суб’єктів функціональних елементів та/або наявні всі типи користувачів та всі типи процесів, на які поширюється політика ФПБ. [3]
Здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта	ФБО повинні реалізовувати керування доступом до об’єктів, що ґрунтується на списку суб’єктів та об’єктів та дозволяти доступ що ґрунтується на атрибутах безпеки, які явно дозволяють доступ. Повинні дозволяти інформаційний потік між керованим суб’єктом та керованою інформацією за допомогою керованої операції.	В атрибутах безпеки функціональних елементів наявні атрибути процесів та об’єктів усіх типів, на які поширюється політика ФПБ, що дозволяють керувати операціями переміщення інформації від об’єктів відповідних типів до процесів відповідних типів (операціями читання інформації).

Таблиця 2. Відомості щодо зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-9.

Вимоги критеріїв гарантій НД ТЗІ 2.5-004-99	**Вимоги стандарту ISO/IEC 15408-3 щодо елементів компонентів довіри, які у сукупності забезпечують задоволення відповідних вимог НД ТЗІ 2.5-004-99**	**Умови задоволення елементами довіри вимог НД ТЗІ 2.5-004-99**
Розробник повинен визначити всі стадії життєвого циклу ОЕ, розробити, запровадити і підтримувати в робочому стані документально оформлені методики	Розробник повинен визначити модель життєвого циклу, що використовується при розробці та супроводженні об'єкту оцінювання (ОО). Розробник повинен надати документацію з визначення життєвого циклу. Документація містить опис моделі. Модель життєвого циклу має забезпечити необхідний контроль. Документація містить опис моделі. Модель життєвого циклу забезпечує необхідний контроль за розробкою та супроводженням ОО	У моделі життєвого циклу, яка наведена у документації з визначення життєвого циклу, зазначеній в елементах довіри ,документовані всі етапи кожної стадії життєвого циклу ОО і їх граничні вимоги
Розробник повинен описати стандарти кодування, яких необхідно додержуватися в процесі реалізації	Розробник ідентифікує інструментальні засоби розробки ОО. Розробник документує обрані опції інструментальних засобів розробки, що обумовлені реалізацією. Розробник повинен навести опис стандартів реалізації для всіх частин ОО. Усі інструментальні засоби розробки, що використовуються для реалізації, мають бути повністю визначені.	Інструментальні засоби розробки, зазначені в елементах довіри, використовуються для компіляції усіх вхідних кодів ОО. [2]

Потреба в удосконаленні існуючого нормативно-методичного забезпечення ІБ в сформованих інформаційних технологіях і підходах починає розвиватися і виходити на сучасний міжнародний рівень. Цьому свідчить початок гармонізації зі стандартом ISO/IEC 15408 та порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 тощо. На порядку денному - оцінка відповідності за міжнародними стандартами.

Література

1. Грайворонський М. В., Новіков О. М. Безпека Інформаційно-Комунікаційних Систем. – К.: Видавнича група BHV, 2009. – 544-552с.
2. НД ТЗІ 2.6-003-2015 Порядок зіставлення компонентів довіри до безпеки, визначених ISO-IEC 15408, з вимогами НД ТЗІ 2.5-004-99.
3. НД ТЗІ 2.7-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання на відповідність вимогам ISO-IEC 15408 з вимогами НД ТЗІ 2.5-004-99.