Забезпечення порівнянності результатів оцінки захищеності автоматизованих систем

Надія Казакова[1], Юрій Щербина[1],
Олексій Соловйов[2]

1. Кафедра інформаційних систем в економіці,
Одеський національний економічний університет,
УКРАЇНА, м.Одеса, вул.Преображенська, 8
E-mail: kaz2003@ukr.net, scherbina_yura@mail.ru

2. Центр підвищення кваліфікації Одеської філії ОАО
«Укртелеком», УКРАЇНА, м.Одеса, вул.Садова, 10
E-mail: amt@ukr.net

Brief summary – Are reported major problems associated with regulatory support in the field of information security. Analyzed documents allow perform risk analysis in modern computer systems. We present suggestions for the improvement of Ukrainian legal framework for the protection of information in computer systems.

Ключові слова – захищеність автоматизованих систем, аналіз ризиків, параметри погроз.

I. Вступ

Тенденція переходу на безпаперові технології з використанням автоматизованого документообігу та розвиток відкритих глобальних телекомунікаційних систем, вимагає вживання відповідних заходів по захисту інформаційних процесів. Реалізація заходів вимагає точної оцінки діючих у середовищі експлуатації автоматизованих систем (АС) загроз і рівня захищеності їх інформаційних ресурсів. Складність формалізації процесів, що відбуваються в АС, не дозволяє виключити суб'єктивний фактор при використанні для цих цілей різних експертних систем. Проте, це завдання повинне вирішуватися таким чином, щоб власники та користувачі АС були гарантовані від недостовірних оцінок захищеності. З цієї причини в 90-ті роки минулого сторіччя в розвинених країнах світу були розроблені та введені в дію нормативні документи, які регламентують дії розроблювачів та оцінювачів захищених інформаційних технологій (ІТ) і створюваних на їхній основі АС.

II.Актуальність проблеми

Питання про необхідність законодавчого забезпечення діяльності, пов'язаної з захистом інформації, стало практично відразу ж, як тільки для її обробки почали застосовувати розподілені обчислювальні системи.

Значна робота в цій області проводилася і в нашій країні. В 1999 був прийнятий документ за назвою «Критерії оцінки захищеності в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 2.5-004-99) [1], який регулює діяльність по захисту інформації в комп'ютерних системах, а також пакет супутніх йому нормативних документів, які діють дотепер [2-5]. Комп'ютерна безпека за останні перетворилася самостійну галузь знань, а швидкі темпи розвитку відкритих телекомунікаційних систем змусили найбільш розвинені країни Західної Європи та США об'єднати свої зусилля з метою узагальнення накопиченого в цій сфері досвіду. Вони розробили ряд міжнародних документів, які дозволяють здійснювати достовірну оцінку захищеності сучасних АС.

Прийняття міжнародних нормативних документів в області захисту інформації, ставить перед вітчизняними розроблювачами завдання, суть якого полягає в приведенні національної нормативно-правової бази у відповідність із їхніми вимогами. Іншим, не менш важливим завданням є розробка відповідних методик і інструментальних засобів оцінки захищеності АС. Відповідно, метою доповіді є висвітлення наявних розбіжностей у напрямках розвитку між світовою та вітчизняною нормативно-правововими базами в області захисту інформації в АС і шляхів їх усунення.

III.Обговорення проблеми

Невідповідність багатьох положень нормативно-правових документів України, які регламентують рішення питань, пов'язаних з інформаційною безпекою сучасним вимогам, не дозволяють вітчизняним розроблювачам використовувати результати оцінок інформаційних технологій, що отримані фахівцями інших країн. Більше того, за час, що пройшов з моменту приймання документів НД ТЗІ 2.5-004-99 та [4], архітектура сучасних розподілених обчислювальних систем та мереж, значно змінилися у бік їх ускладнення. За цей час ISO прийняла цілий ряд документів аналогічного змісту, які акумулюють накопичений досвід. Найбільш значимим з них є міжнародний стандарт ISO 15408 [6-8]. У ньому найбільш повно представлені критерії оцінки механізмів безпеки програмно-технічного рівня. Використання цього документа дозволяє оцінити рівень захищеності автоматизованої системи з погляду повноти реалізованих у ній функцій безпеки, а також надійності їх реалізації. Разом з зазначеними документами був опублікований ряд інших, які їх доповнюють. Це «Загальна методика оцінки безпеки ІТ», «Посібник з проведення сертифікації та акредитації комп'ютерної безпеки», «Профілі захисту для міжмережевих екранів та комерційних систем» та ряд інших, які у вітчизняній літературі іменуються загальною назвою «Єдині критерії».

Зараз можна говорити про створення єдиної мови для формулювання тверджень щодо безпеки АС (вимог, загроз та цілей захисту), а також часткової формалізації цієї предметної області. Розробка концепцій, які б базувалися на вище зазначених, дозволило б підвищити ефективність проведення відповдних оцінок та якість одержуваних результатів. Крім того, це дозволило б використовувати накопичений світовим співтовариством досвід у предметній області. Зокрема, уже зараз можна порівнювати між собою результати сертифікаційних випробувань, отриманих у рамках єдиної схеми. Єдині критерії дозволять підтримувати сумісність з уже існуючими документами та, як уже зазначалося, дозволять розробникам АС використовувати власний, накопичений у роботі, досвід, який буде корелюватися з досвідом зарубіжних розробників.

Завдання, розв'язувані в рамках Єдиних критеріїв, на території України регламентуються документом НД ТЗІ 2.5-004-99. Цей документ, як і Єдині критерії, визначає функціональні вимоги безпекита вимоги до адекватності реалізації функцій безпеки. Однак тлумачення аналогічних термінів у зазначених документів не завжди збігається. І, найголовніше, ступінь деталізації вимог до функцій безпеки та вимог до адекватності їх реалізації, помітно відрізняється. Так, наприклад НД ТЗІ 2.5-004-99 містить тільки чотири групи вимог до безпеки загроз (конкретно викладені у доповіді). Що стосується Єдиних критеріїв, то до їхнього складу входить одинадцять функціональних класів, що визначають функції захисту. При цьому кожний клас включає ряд сімейств, які, у свою чергу, діляться на компоненти, а компоненти на елементи. Вимоги в межах кожного сімейства відрізняються акцентами або строгістю. Сам зміст класів помітно відрізняється від пропонованої НД ТЗІ 2.5-004-99 класифікації. Зокрема, функції захисту в них розділені відповідно до інших класифікаційних ознак. До них ставляться: «аудит», «криптографічна підтримка», «зв'язок», «захист користувача», «ідентифікація та аутентифікація», «керування безпекою», «приватність», «захист функцій безпеки об'єкта оцінки», «використання ресурсів», «доступ до об'єкта» і «довірений канал/маршрут». Ця відмінність відзначає явну користь Єдиних критеріїв та невідповідність їм НД ТЗІ 2.5-004-99.

Є достатньо принципові відмінності, які обумовлені відмінностями в розумінні терміна «загроза». Так, у НД ТЗІ 2.5-004-99 на перше місце ставиться інформаційний об'єкт, що захищається, і наслідки від реалізації погрози, а саме – втрата однієї з властивостей інформації. У Єдиних критеріях головним визнаються вразливі місця в системі захисту та способи її подолання. Цим пояснюється різноманітність класів, на які розділені пропоновані у документах функціональні вимоги безпеки та їх кількість. Фактично, Єдині критерії пропонують визначати слабкі місця в захисті, а потім з'ясовувати які ресурси системи це наражає на небезпеку та у якому ступені. Очевидно, така модель є більш ефективною, оскільки результуючий досвід у цій сфері базується на статистичному аналізі атак. Саме тому назви класів охоплюють усі аспекти захисту: від її організації та перевірки адекватності загрозам до контролю інформаційних потоків.

Широкий спектр функціональних послуг захисту, пропонований у Єдиних критеріях, дозволяє протистояти більшому числу загроз і будувати більш гнучкі системи захисту. Вимоги довіри до безпеки також мають більш широкий спектр. Вони розділені на вісім класів, кожний з яких має багаторівневу ієрархічну структуру. Зокрема, оцінку рівнів довіри до реалізованої системи безпеки передбачається проводити по таких напрямках як «керування конфігурацією», «поставка та експлуатація», «розробка», «підтримка циклу», «тестування», «оцінка уразливостей» та «підтримка довіри». По своєму складу ці напрямки ширше й більш глибоко деталізують заходи, які пов'язані з визначенням гарантій захисту.

Нарешті, у Єдиних критеріях більш глибоко прописані залежності між окремими компонентами функціональних вимог безпеки та вимог до адекватності їх реалізації.

Крім зазначеного, у доповіді відмічається необхідність кореляції понять та, відповідно, розробка управляючих дій, які викладені у [9] та вітчизняному документі НД ТЗІ 1.4-001-2000 [10]. Відмічається, що вітчизняний документ по своєму змісту програє стандарту ISO/IEC 17799, так як у ньому містяться самі загальні визначення та відсутня детальна інформація про те, як на практиці здійснювати діяльність, пов'язану з проектуванням, експлуатацією та управлінням захищеними автоматизованими системами.

Висновок

Відмітимо, що відмінність у підходах до захисту інформації, яка склалася на теперішній час і яка закладена у нормативній базі України та нормативній базі більшості країн з розвиненими інформаційно-телекомунікаційними системами, гальмує розвиток технологій оцінки захищеності АС, обмежуючи застосування тих з них, що апробовані та одержали поширення за кордоном. Саме на подолання розбіжностей необхідно спрямовані зусилля вітчизняних фахівців в області інформаційної безпеки.

Література

[1] НД ТЗІ 1.1-003-99. Критерії оцінки захищеності в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.

[2] НД ТЗІ 1.1-003-99 Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.

[3] НД ТЗІ 1.1-002-99 Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.

[4] НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України.

[5] НД ТЗІ 3.7-001-99 Методичні вказівки по створенню технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

[6] Information technology. Security techniques. Evaluation criteria for IT security. Part 1 : Introduction and general model. – ISO/IEC 15408-1.1999.

[7] Information technology. Security techniques. Evaluation criteria for IT security. Part 2 : Security functional requirements. – ISO/IEC 15408-2.1999.

[8] Information technology. Security techniques. Evaluation criteria for IT security. Part 3 : Security assurance requirements. – ISO/IEC 15408-3.1999.

[9] Information technology. Security techniques. Code of practice for information security management. – ISO/IEC 17799-2005.

[10] НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.