

В'ячеслав Ковтун, Марія Юхимчук, Дмитро Олійник (Вінниця)

МОДЕЛЮВАННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ КРИТИЧНОГО ЗАСТОСУВАННЯ

Порівняно із універсальними інформаційними системами [1], інформаційна система критичного застосування має спрощену структуру інформаційного середовища і специфічні вимоги щодо обсягів і характеру інформаційних ресурсів. Це факт дозволяє відмовитися від надмірної деталізації і звузити об'єкт моделювання до процесу формування політики безпеки інформаційної системи критичного застосування, адекватний проблемний опис якого є досяжним за умови раціонального вибору математичного апарату. Отже, метою проведених досліджень був синтез математичного апарату для комплексного уніфікованого опису статичних і динамічних, контрольованих за цілісністю та автентичністю, процесів у інформаційній системі критичного застосування у її ієрархічному представленні.

Автори отримали нові комплексні математичні моделі процесів оброблювання інформації та розмежування доступу до неї, які, на відміну від існуючих, описують в рамках математичного апарату Е-мереж механізми забезпечення середовища та ресурсів інформаційної системи критичного застосування і дозволяють кількісно оцінити цілісність її інформаційних ресурсів. Розроблено математичні моделі синтезу політики безпечної взаємодії інформаційних процесів у інформаційній системі критичного застосування, які дозволяють гарантувати дотримання локальних політик безпеки на різних структурних елементах системи і інтегрувати їх у глобальну політику безпеки із дотриманням єдиної дискреційної політики скрізь у системі.

Практичним наслідком отриманих автриами теоретичних результатів стали методи оптимізації роботи блоків оброблювання даних і розмежування доступу, які відповідають у інформаційній системі критичного застосування за контроль цілісності інформації та автентичність доступу до неї відповідно. Зокрема, формалізовано асоційований із моделлю політики безпеки інформаційної системи критичного застосування, адаптований для практичного застосування, метод динамічного контролю цілісності інформації із відповідним критерієм, який базується на математичному апараті напівмарковських мереж для комплексного стохастичного опису дискретних станів контролю цілісності інформації на вибраних ієрархічних рівнях системи під час неперервного дискреційного доступу. Метод дозволяє вибрати максимальні допустимі значення коефіцієнтів контролю цілісності інформації на підрівнях прикладного рівня OSI, виділених у інформаційній системі критичного застосування, на основі попередньо заданого обсягу контрольованої інформації, швидкості контролю її цілісності та максимальної тривалості перебування системи у відповідному стані. Також представлено метод контролю доступу до системних інформаційних процесів відповідними комплексами інтегрованих множин класифікаторів, які фіксують факти перевищення відповідних порогових значень зваженими ступенями ідентичності атрибутів об'єкту, який бажає отримати доступ, відомим класам інформаційних загроз, що ініціює описану у системній політиці безпеки реакцію. Аналіз результатів проведених експериментів дозволив одержати оптимальні параметри груп класифікаторів, які, в рамках глобальної, локальної та дискреційної політик безпеки, запобігають отриманню несанкціонованого доступу до системних інформаційних ресурсів або спробам порушення їх цілісності.

Висновки. Вперше представлено математичну модель інформаційної системи критичного застосування, у якій, на відміну від існуючих, запроваджено єдиний підхід для опису інформаційних процесів в рамках глобальної, дискреційної і локальної політик безпеки із прив'язкою до ієрархічної структури інформаційної системи, що дозволяє виконувати аналіз і синтез функцій сервісів підтримки ролей користувачів на основі об'єктно-реляційною моделі організації системи управління інформацією із можливістю їх інтеграції, індукування та сумісності в межах єдиної політики безпеки, контролювати цілісність інформації та автентичність статичного і динамічного доступу до неї.

Література

1. Conceptual Modeling of Information Systems [Electronic resource]. - Access mode: <http://infocat.ucpel.tche.br/disc/mc/cmis.pdf>.