УДК 335.01

ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВИНИКНЕННЯ КОНФЛІКТУ

А. В. Дудатьєв, к.т.н., доцент
О. П. Войтович, к.т.н., доцент
Вінницький національний технічний університет
andreysaf60@mail.ru

Створення глобального інформаційного середовища принципово змінило технології використання інформаційних ресурсів та їх взаємозв'язок з різноманітною діяльністю людини. У зв'язку з цим актуальною є задача оцінювання та забезпечення інформаційної безпеки, яка напряму впливає на всі інші види безпеки, зокрема, економічну, техногенну, екологічну тощо. Проблема оцінювання та забезпечення інформаційної безпеки виникає, як наслідок конфлікту, у результаті виконання певних дій з метою несанкціонованого доступу до конфіденційних інформаційних ресурсів. Характерними особливостями таких конфліктів є:

- несанкціонований доступ до інформаційних ресурсів змінює взаємодію між суб'єктом (конкурентом) системи і об'єктом захисту;
- у процесі отримання конфіденційної інформації мета суб'єкта та його спеціальні засоби можуть змінюватись;
- процес отримання конфіденційної інформації, а також ймовірні протидії є у великій мірі невизначеними.

Проблема оцінювання та забезпечення рівня необхідної інформаційної безпеки формулюються, як дві класичні задачі аналізу та синтезу ефективної системи

захисту, які вирішуються як на етапі проектування системи захисту інформації (СЗІ), так і на етапі її експлуатації. Ці задачі пропонується вирішувати комплексно, що формалізується у таких кроках:

- ідентифікація існуючих та ймовірних загроз;
- розробка математичної моделі для оцінювання рівня захищеності об'єкту;
- розробка політики інформаційної безпеки (ПІБ) з урахуванням результатів моделювання;
- синтез оптимальної СЗІ.

Для отримання більш ефективного результату на етапах моделювання, розробки ПІБ і синтезу СЗІ пропонується враховувати, як елемент системи – інформаційно-аналітичну підсистему (ІАП). Результати діяльності ІАП використовуються для підготовки відповідних управлінських рішень які спрямовані на випередження певних дій ймовірних конкурентів та мінімізацію ризиків. Більшість конфліктних ситуацій характеризуються невизначеністю, зокрема, параметричною та процедурною. Це накладає певні особливості щодо використання адекватного математичного апарату для моделювання стану об'єкту захисту на різних етапах його життєдіяльності, та формулює оригінальні задачі, які пов'язані із забезпеченням необхідного рівня безпеки з урахуванням та упередженням дій конкурентів.

У доповіді пропонуються математичні моделі для оцінювання рівня захисту інформаційної безпеки та синтезу СЗІ в умовах конкуренції або конфліктної ситуації. Запропонована математична модель функціонування ІАП за умов виникнення потенційної конфліктної ситуації, дозволяє виконати вибір безконфліктних операцій, зокрема, операцій або дій відносно ресурсів, дозволяє забезпечити стійкість взаємодії об'єкту захисту із оточуючим конкуруючим середовищем.