УДК 004.056

О.С.Потенко

Інститут проблем моделювання в енергетиці ім. Є.Пухова, Київ

РОЗРОБКА МЕТОДИКИ ВИБОРУ СКЛАДУ ПРОФІЛЮ ПРОТИДІЇ ЗАГРОЗАМ НА ОСНОВІ АНАЛІЗУ ВІРОГІДНОСТІ ЇХ РЕАЛІЗАЦІЇ

Проблема інформаційної безпеки в інформаційно-телекомунікаційних системах (ІТС), та побудови комплексних систем захисту інформації (КСЗІ) останнім часом привертає все більш серйозну увагу з боку фахівців, особливо, якщо таку систему використано на об’єктах критичної інфраструктури. Комплексна система захисту інформації – це сукупність організаційних та інженерно-технічних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

Необхідність створення КСЗІ в ІТС регламентується законодавством України. Оцінити наявність послуг безпеки в комп'ютерній системі дозволяють функціональні критерії, а критерії гарантій дозволяють оцінити коректність реалізації послуг. Щоб задовольняти певним вимогам захищеності інформації, яка обробляється в ІТС, комплекс засобів захисту (КЗЗ) обчислювальної системи повинен відповідати профілю захищеності, що являє собою перелік мінімально необхідних рівнів послуг.

З метою перевірки, аналізу та оцінки КСЗІ ІТС щодо їх відповідності вимогам нормативних документів з технічного захисту інформації та можливості їх використання для забезпечення технічного захисту інформації (далі - ТЗІ) проводиться державна експертиза у сфері технічного захисту інформації.

Однією із наукових задач яка вирішується для забезпечення процедури проведення державної експертизі у сфері технічного захисту інформації це вибір методу побудові складу профілю протидії загрозам на основі аналізу вірогідності їх реалізації

Для вирішення задачі проектування профілів, адаптивних загрозам за підкласами АС, пропонується використовувати метод динамічного програмування. Використовуючи класичний підхід [1], можна розробити прикладний алгоритм (методику) оцінки профілів, адаптивних загроз за підкласами автоматизованих систем

АС-1, АС-2, АС-3, на кроки, на кожному із яких склад профілю буде покращено. Для цього необхідно провести дослідження реалізації вимог НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99 та визначити прикладний фізичний зміст, що дозволить розробити методику обчислення параметрів цільової функції під час оптимізації.

Крок 1: Введення початкових значень

Крок 2: Розрахунок цільової функції апроксимованого виду для n об'єктів

Крок 3: Знайти максимальне значення математичного очікування втрат на перших n об'єктах АС

Крок 4: Порівняти значення математичного очікування втрат із початковим. Якщо воно більше, то перейти к пункту 6. Якщо ні, то – до кроку 5.

Крок 5: Прийняти N=N+1 та перейти до кроку 2.

Крок 6: Знайти розподіл атакуючих потенційних загроз по n об'єктах захисту.

Розроблено програмне забезпечення для реалізації методики обчислення параметрів цільової функції під час оптимізації, яке за рахунок використання методу динамічного програмування надає можливість реалізувати принцип оптимальності Р. Беллмана: з якого б етапу ми не почали визначати новий склад профілю для протидії загрозам в залежності від наявності ресурсів захисту щодо апаратного та програмного забезпечення (модернізація, удосконалення, переоснащення, нова політика безпеки тощо), то всі подальші етапи будуть більш оптимальними.

Тестування програмного забезпечення дозволило отримати аналітичні залежності для різних профілів протидії загрозам, що дозволяє оптимізувати процедуру вибору профілю в залежності від вимог до інформації яка обробляється.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Richard E. Bellman. Dynamic Programming. - Princeton University Press, 2010. – 392 p.