сервери, комутатори, маршрутизатори та ін.), так і програмні (операційні системи, програми, бази даних та ін.) компоненти. Також розглядається поняття відмовостійкості системи, тобто здібності сервера, мережевої інфраструктури або центру обробки даних в найкоротші терміни відновити роботу після збою.

Література

1. Віто А. Основи організації мереж Cisco. Том 2. / Віто А. – М.: Альпина Паблишер, 2006. – 464 с.

2. Телекомунікаційні системи та мережі / Шувалов В. П., Величко В. В., Субботін Е. А., Ярославцев А. Ф., 2005. – 336 с.

3. Основні аспекти якості телекомунікаційних послуг. http://mybiblioteka.su/10-37676.html

УДК 004.056

ОЦІНКА ЗАХИЩЕНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

к.т.н., с.н.с. Гроза П.М., Варига А.В.

Полтавський національний технічний університет
імені Юрія Кондратюка, Полтава

Інформація є одним з основних ресурсів науково-технічного і соціально-економічного розвитку суспільства, а тому питання її захисту є першочерговим.

Основними причинами низької захищеності комп'ютерних мереж є: недосконаліть стеку протоколів TCP/IP, складність адміністрування неоднорідних мереж, помилки адміністраторів та користувачів, уразливості програмного забезпечення.

Забезпечення безпеки функціонування роботи мережі представляє собою безперервний процес рішення адміністратором безпеки послідовності виникаючих задач.

Для контролю захищеності комп'ютерної мережі адміністратором безпеки використовуються системи аналізу захищеності (сканери безпеки). Суть роботи системи аналізу захищеності полягає у виконанні серії дистанційних тестів з виявлення вразливостей. В умовах дефіциту часу і великої щільності потоку задач, які потребують вирішення, однією з важливих вимог діяльності адміністратора є зменшення часу рішення задач, які на нього покладені. В якості однієї з проблем, які виникають у таких системах, є проблема підвищення творчого потенціалу людини за рахунок оптимальної організації його роботи.

Аналіз роботи адміністратора безпеки при визначені стану захищеності комп'ютерної мережі показує, що етап інформаційної підготовки прийняття рішення займає більшу частину від кількості всіх операцій, які виконуються при цьому.

Запропонована методика оцінки захищеності комп'ютерної мережі на основі логіко-лінгвістичного підходу та апарату нечіткої логіки забезпечує обробку експертної інформації, яка зберігається в базі знань. База знань формується на основі знань фахівців предметної області, як безліч нечітких правил і забезпечує побудову пропозицій на прийняття рішення по аналізу захищеності мережі аналогічно діям, що звичайно виконує досвідчений адміністратор безпеки у відповідних умовах.

Основними критеріями якості контролю захищеності комп'ютерної мережі є повнота контролю та його періодичність. Підвищення повноти контролю досягається за рахунок врахування поточного стану мережі та доступності вузла для контролю. В свою чергу скорочення періоду контролю досягається за рахунок його безперервності та виключення ручних підготовчих операцій.

За допомогою розробленої програми було проведене імітаційне моделювання роботи системи аналізу захищеності мережі. На основі результатів моделювання проведена оцінка ефективності запропонованої методики.

Література

1. Мэйволд Э. Безопасность сетей. //2-е изд., исправленное. – М.: Интуит, 2016. – 571с.

2. Сахно В.В. Применение методов нечеткой логики для решения задачи обеспечения информационной безопасности. [Електронний ресурс] – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/primenenie-metodov-nechetkoy-logiki-dlya-resheniya-zadachi-obespecheniya-informatsionnoy-bezopasnosti.

3. Спецификация: безопасность конечных точек. Symantec™ Network Access Control. [Електронний ресурс] – Режим доступу до ресурсу: https://www.symantec.com/content/ru/ru/enterprise/fact_sheets/b-datasheet_nac_11.pdf.

УДК 004.056.5

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЯК ФУНКЦІОНАЛЬНА ПІДСИСТЕМА ОБ'ЄКТУ ІНФОРМАТИЗАЦІЇ

к.т.н., доцент Дегтярьова Л.М.

Полтавський національний технічний університет
імені Юрія Кондратюка, Полтава
E-mail: ladegt12@gmail.com

Рівень інформаційної безпеки сьогодні багато в чому визначається процесом інформатизації сучасного світу, і, як наслідок, необхідністю різнопланового захисту інформації, незалежно від місця знаходження її носіїв; широке використання в органах управління спеціалізованих і глобальних інформаційних систем, що накопичують і передають величезні обсяги цінної інформації і, в той же час, вразливих для неконтрольованого доступу до інформації, що захищається, зростання ризику і небезпеки несанкціонованих впливів на інформацію в цих системах; відносно велика величина небезпеки