розсиланні електронних повідомлень із метою крадіжки конфіденційної інформації (як правило, фінансового характеру).

Фішинг-повідомлення складаються таким чином, щоб максимально походити на інформаційні листи від банківських структур або компаній з відомими брендами. Листи містять посилання на свідомо помилковий веб-ресурс, спеціально підготовлений зловмисниками і є копією сайту організації, від імені якої відправлений лист.

На даному фальшивому сайті користувачеві пропонується ввести, наприклад, номер своєї кредитної карти й іншу конфіденційну інформацію.

Отже, розробка програмного забезпечення системи формування фільтрів від фішингу в мережі Internet є актуальною задачею, яка потребує розв'язку.

Список літератури

1. Гайкович В., Першин А., Безопасность электронных банковских систем. – Москва.: Единая Европа, 2002.
2. Галатенко В., Информационная безопасность, «Открытые системы». – М.: Азбука-Книга, 2005.

УДК 004.4

В.В. Джебко
Науковий керівник – Сидоренко В.В., ст. викладач
Кіровоградський національний технічний університет

Програмне забезпечення системи контролю та керування доступом з використанням смарт-карт за технологією RFID

Принцип комплексного «інтелектуального» управління всіма життєво важливими функціями житлових і промислових об'єктів, практична реалізація якого стала можливої завдяки застосуванню інтегрованих слабкострумових систем, знаходить сьогодні все більшу популярність.

Особливе значення при цьому мають спеціальні програмно-апаратні комплекси, призначені для забезпечення безпеки, і, насамперед, – системи контролю й управління доступом, або, скорочено СКУД.

Що являють собою системи контролю доступу? Загалом їх можна охарактеризувати як призначені для здійснення контролю й управління доступом як безпосередньо на об'єкт у цілому, так і на його окремі ділянки, комплекси, що поєднують у своєму составі організаційно-адміністративні заходи й великий перелік програмно-технічних засобів.

Крім властиво управління доступом з метою попередження проникнення на об'єкт небажаних осіб, функція системи контролю доступу може полягати також у спостереженні за обслуговуючим персоналом, включаючи пересування в межах території об'єкта, моніторинг періоду перебування на робочому місці, раціональність використання робочого часу й т.д. Установка систем контролю доступу й у житлових приміщеннях не менш затребувана, чим на господарських об'єктах, просто домашні системи, як правило, відрізняються більшою простотою й меншою кількістю інтегрувальних у їхній состав функціональних елементів.

Таким чином, виходячи з вищеперерахованого, розробка програмного забезпечення системи контролю та керування доступом з використанням смарт-карт за технологією RFID є актуальною задачею.

Список літератури

1. Автоматизированная Система Контроля Доступа SmartMonitor Plus V1.1.0/ Руководство пользователя. Минск.
2. О системах контроля доступа. М.: ТЕХИНВЕСТ – 2004 http://www.sistema-dostupa.ru
3. Системы управления доступом. М.: ТЕХИНВЕСТ – 2004 http://www.sistema-dostupa.ru
4. Требования разработки и внедрения СКД. М.: ТЕХИНВЕСТ – 2004 http://www.sistema-dostupa.ru
5. ПЗ для систем контроля доступа. М.: ТЕХИНВЕСТ – 2004 http://www.sistema-dostupa.ru

УДК 004.725.4

Д.І. Кулик
Науковий керівник – Павлик С.І., канд. фіз.-мат. наук, доцент
Запорізька державна інженерна академія

Масштабно-інваріантна поведінка процесу зростання комп’ютерних мереж

Еволюція складних мереж та розповсюдження сигналів нею останнім часом обґрунтовано привертає велику увагу з точки зору можливого застосування до аналізу усесвітньої павутини (World Wide Web), яка трактується як розподілена система, що надає доступ до зв'язаних між собою документів, розташованих на різних комп'ютерах, підключених до Інтернету [1]. Крім того, такі складні мережі описують різні системи, що зустрічаються в природі і суспільстві. За традицією ці системи моделюються як випадкові графи з відносно примітивною і жорсткою структурою. Але ці моделі не завжди демонструють топологічні і структурні властивості, що відображуються в реальних прикладах мереж. Це пов'язано з певною обчислювальною складністю при їх комп'ютерному моделюванні. Основна проблема - виявити закономірності в поведінці складної мережі при зміні її масштабу. Для цього існує розвинений теоретичний підхід, пов'язаний з масштабно-інваріантними властивостями складних систем (так званий скейлінг).

Вживання концепції скейлінга для моделювання поведінки випадкових мереж вже обговорювалася в ранній роботі [2]. Проте, складність моделювання випадкових систем заставляє шукати простіші моделі, на основі аналізу яких можна відповісти на низку запитань, які виникають в реальній поведінці, наприклад, усесвітньої павутини. Для цієї мети ми використовуємо модель ZRP (zero-range process) [3] разом із спробою інкорпорувати в неї концепцію скейлінга. Основні особливості використання моделі ZRP в нашому завданні полягають в наступному. Уявимо собі одновимірний ланцюжок з певним числом вузлів L, у вузлах якого може знаходитися довільне число частинок $h(x,t)$, де x - номер вузла від початку, t - час. На перший вузол частинка заходить з вірогідністю p, з останнього вузла вирушає з вірогідністю q. Між вузлами частинки здійснюють переходи з вірогідністю $u(h)$. Завдання полягає в обчисленні $W(L,t) = \sqrt{\langle [h(x,t) - \langle h(x,t)\rangle]^2\rangle}$, де $\langle h(x,t)\rangle = e\ h(x,t)/L$, сумування - по вузлах x. Ґрунтуючись на даних математичного моделювання і на аналогії з масштабно-інваріантними законами в теорії фазових переходів, раніше (див. [4-5]) запропоновано