

процесора, таймера ОС, годинника реального часу. Основну роль в цьому процесі відіграють інтервальний таймер, RTC та таймера ОС. Саме емуляція їх роботи повинна бути в повній мірі доступна користувачеві як у програмуванні, так і відображенні всіх внутрішніх процесів функціонування цих пристроїв.

Список літератури

1. Сидоренко В.В. Використання програмних емуляторів пристроїв обчислювальної техніки в навчальному процесі. / В.В. Сидоренко, О.В. Коваленко, О.П. Доренський. // Матеріали III Міжнар. НТК "Комп'ютерні системи та мережні технології". – К.: НАУ, 2010. – С. 89.
2. Гуржій А.М., Коряк С.Ф., Самсонов В.В., Склярів О.Я. Архітектура, принципи функціонування та керування ресурсами IBM PC: Навч. посіб.. – Х.: ТОВ "Компанія СМІТ", 2003. – С. 247-279.
3. Валова К.М. Програма-емулятор системного таймера. / К.М. Валова // Збірник тез XLI наукової конференції студентів і магістрантів Кіровоградського національного технічного університету. Кіровоград: РВЛ КНТУ, 2007. – С. 65.
4. Гуртовий Є.О. Програма-емулятор годинника реального часу (RTC) на платі IBM PC. / Є.О. Гуртовий // Збірник тез XL наукової конференції студентів і магістрантів Кіровоградського національного технічного університету. Кіровоград: РВЛ КНТУ, 2006. – С. 66.
5. Захарова І. Г. Інформаційні технології в освіті: Навчальний посібник – К.: Академія, 2003. – 192 с.
6. Мельниченко Т.М. Програмний емулятор системного та реального часу на платі IBM PC в навчальному процесі підготовки системних програмістів. // Матеріали III Міжнар. науково-технічної конференції "Комп'ютерні системи та мережні технології" (CSNT-2010). – К.: НАУ, 2010. – С. 73.

Розробка програмного забезпечення топологічного проектування та балансування навантаження трафіку у мережі

О.С. Первий, студент,
О.А. Смірнов, доцент, канд. техн. наук,
Є.В. Мелешко, ст. викладач, канд. техн. наук
Кіровоградський національний технічний університет

З початку нового тисячоріччя усе виразніше простежується тенденція подорожчання переданої й збереженої в обчислювальних мережах інформації. Все частіше з'являються твердження про те, що вартість даних перевищує не тільки витрати по організації зв'язку, але й усього програмно-апаратного комплексу й використовуваних обчислювальних засобів. Це пов'язане з бурхливим розвитком електронного документообігу, що одержав крім потужної технологічної й технічної бази ще і юридичну підтримку. Крім державного сектора, що активно використовує ця можливість для організації захищеного каналу зв'язку між різними департаментами й службами, ще більш швидкими темпами росте ІТ-сектор корпоративного захищеного документообігу. Інвестиції в цю технологічну область зараз вважаються одними із самих швидкоокупаємих й перспективних.

Природно припустити, що коштвна інформація вимагає безвідмовних і надійних методів її захисту. На сучасний момент і служби інформаційної безпеки державних установ і їхні комерційні аналоги чітко усвідомили необхідність використання більше комплексного й надійного засобу захисту, ніж міжмережний екран і антивірусний засіб, що проте не має на увазі відмову від використання цих

засобів. Для комплексного захисту документообігу всі частіше використовується технологія Удостоверюючих Центрів, базована на концепції Інфраструктури Відкритих Ключів (ІВК). Остання, у свою чергу, заснована на криптографічних поняттях, методах і теоріях, об'єднаних у єдину систему для практичного застосування.

Метою роботи є створення методу динамічної адаптації навантаження на компоненти мережі УЦ, а також розробка алгоритму побудови оптимальної топологічної структури мережі із Удостоверюючим Центром.

Об'єктом дослідження є процес підвищення якості функціонування мережа з УЦ шляхом оптимізації й реконфігурації її топологічної структури, а так само динамічного керування інформаційним потоком.

Предметом дослідження є аналітичні й імітаційні моделі, які формалізують процес генерації й трансляції інформаційного потоку в мережі з УЦ із обліком її топологічних особливостей і набору вхідних параметрів.

Методи дослідження. У процесі моделювання використовується комплексний системний підхід, методи структурного й системного аналізу, теорії графів і теорії масового обслуговування.

Наукова новизна роботи виражається в наступному:

1. На підставі проведеного аналізу обґрунтовані вибір і запропонована структура розподіленої мережі з УЦ.

2. Розроблено функціональну модель мережі з УЦ, що дозволяє визначити взаємозв'язок між інформаційними потоками й провести функціональну декомпозицію системи.

3. Розроблено евристичний алгоритм пошуку оптимальної топологічної структури мережі з використанням запропонованого критерію оптимізації й обмежень, що розраховуються на основі наведених витрат і ймовірно-тимчасових характеристик.

4. Запропоновано інтегральний критерій оптимізації системи адаптивного балансування навантаження на УК УЦ.

5. Запропоновано метод адаптивного балансування навантаження на УК УЦ на основі матричного підходу, доповнений використанням матриць транзитних шляхів.

Практична цінність роботи виражається в наступному:

1. На основі створених математичних моделей і алгоритмів розроблений програмний модуль (система адаптивного балансування), що доповнює базову функціональність Удостоверюючого Центру, можливістю моніторингу й перерозподілу навантаження на вузли мережі.

2. Результати імітаційного моделювання, оформлені у вигляді програмного модуля зі зручним користувальницьким інтерфейсом, дозволяють згенерувати вхідний інформаційний потік і реакцію на нього з боку УК УЦ із урахуванням параметрів швидкодії, які задаються, поточної завантаженості й надійності роботи, що робить його придатним для використання в відлагоджувальних цілях на реальних діючих мережах з УЦ.

3. Розроблений алгоритм адаптивного балансування навантаження на УК УЦ застосовується в програмно-апаратному комплексі криптографічного захисту інформації, створеному з урахуванням результатів досліджень, проведених у магістерській роботі.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.