Розробка програмного забезпечення системи виявлення вторгнення у мережу на основі часового аналізу

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

Активне використання, в сучасний час, розподілених систем зв'язку приводить до необхідності приділяти увагу питанням безпеки.

Особливе місце, в реалізації політики безпеки організації, займають системи виявлення вторгнень (подій з безпекою) (СВВ), які можуть, як виконувати функцію зворотного зв'язка, контролюючи ефективність компонентів системи безпеки, тобто бути доповненням до існуючого комплексу засобів захисту, так і являти собою самостійний продукт.

Впровадження багатьох СВВ, як і комплексних систем безпеки, стримується рядом факторів, таких як одноразові капіталовкладення, необхідність компетентної установки, настроювання, підтримки й т.д. У таких компаніях, як правило, функція спостереження за роботою мережі покладає на адміністратора. У такому випадку результат залежить від людського фактора, що включає досвід, інтуїцію, відповідальність, працездатність і т.п. Слід зазначити, що практично в кожній компанії, що має в розпорядженні розподілену мережу, установлені засоби збору статистичних даних про завантаження інтерфейсів мережного встаткування. Таким чином, закономірним кроком до автоматизації процесу виявлення позаштатних ситуацій, є впровадження доступного й, можна сказати, універсального засобу, що аналізує інтенсивності потоків даних у пошуку незвичайних і підозрілих подій або тенденцій, яке можна віднести до підкласу СВВ.

Метою роботи є розробка підвищуючого безпеку функціонування мережі методу виявлення аномалій у даних про завантаження інтерфейсів телекомунікаційного встаткування, на основі аналізу частотних характеристик; оптимізація по обчислювальному навантаженню формуючих метод зсувних спектральних і спектрально-часових алгоритмів з одержанням математичних моделей оптимізації й дослідження особливостей і обмежень використання частотного подання в розглянутому додатку.

Об'єктом дослідження є процес виявлення вторгнення в мережу.

Предмет дослідження – виявлення аномалій у даних про завантаження інтерфейсів телекомунікаційного встаткування.

Методи дослідження базуються на теорії ймовірностей і математичної статистики, теорії розпізнавання образів, теорії обчислювальних систем і мереж.

Наукова новизна положень, що виносяться на захист, полягає в наступному:

Визначено частотні образи для подання особливостей у даних про інтенсивності телекомунікаційних потоків і розроблений алгоритм їхнього виявлення у вейвлет-спектрі сигналу.

Запропоновано математичні моделі оптимізації обчислення спектральних подань, у тому числі для зсувної послідовності.

Виконано дослідження областей вірогідності й невірогідності на картині коефіцієнтів вейвлет-розкладання залежно від довжини аналізованої послідовності й обраного вейвлета.

Запропоновано математичні моделі оптимізації обчислення спектрального подання, у тому числі для зсувної послідовності, з урахуванням області вірогідності коефіцієнтів розкладання.

1. Запропоновано спосіб розрахунку довірчого простору вейвлет-коефіцієнтів поза площиною правдоподібності для можливості їх обґрунтованого включення в подальший аналіз із певним ступенем упевненості.

Практична значимість роботи полягає в розробці описової моделі системи виявлення аномалій у даних про завантаження інтерфейсів мережного встаткування на основі аналізу частотних характеристик, у створенні програмних модулів для реалізації її етапів. Запропоновані моделі оптимізації спектральних і спектрально-часових алгоритмів мають самостійну практичну значимість і можуть знайти застосування в додатках, що передбачають роботу зі спектрами.

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.

Оптимізація розподілення навантаження в комп'ютерній мережі організації

К.В. Калиновська, *студент,*
Є.М. Литвиненко, *викладач*
Харківський національний університет будівництва та архітектури

В сучасному світі жодна область діяльності людини не обходиться без використання інформаційних технологій (ІТ). При чому їх роль з кожним днем становиться все більш значимою в житті сучасного цивілізованого світу. Сьогодні ІТ знищують межі між країнами, роблять суспільство більш відкритим і стимулюють розвиток усіх його галузей. Рівень розвитку ІТ сьогодні – один з найбільш яскравих індикаторів розвиненості регіонів. Багато організацій використовують бази даних, вважають за краще зберігання документів в електронному вигляді, але для більш коректнішої і швидкої роботи організації необхідно створити коректну комп'ютерну мережу.

Комп'ютерна мережа – це сукупність персональних комп'ютерів (ПК) та інших пристроїв (концентраторів, принтерів, модемів і т. д.), об'єднуваних разом за допомогою мережевих кабелів. Пристрої мережі можуть взаємодіяти один з одним з ціллю спільного використання інформації і ресурсів [1].

Найбільш вузьке місце у будь-якій розподіленій комп'ютерній системі — це застаріле устаткування, оскільки максимальна пропускна спроможність комп'ютерної мережі дорівнює максимальній пропускній спроможності її найповільнішого компонента. В цілому, продуктивність комп'ютерної мережі визначається, по-перше, об'ємом інформаційних потоків усередині мережі, по-друге, продуктивністю