

УДК 621.391

*С.В.Індук
S.Indyk*

**СИНТЕЗ ПАРАМЕТРІВ ПРИЙОМО-ПЕРЕДАВАЛЬНОГО МОДУЛЯ
ОПТОВОЛОКОННОЇ СИСТЕМИ ЗВ'ЯЗКУ**

**SYNTHESIS OF PARAMETERS OF THE TRANSCIEIVING MODULE OF A FIBER
OPTIC COMMUNICATION SYSTEM**

До сучасних оптоволоконних систем пред'являються різні техніко-економічні вимоги, які характеризуються сукупністю показників якості. Для відображення повної і об'єктивної інформації про реальну систему необхідно враховувати як технічні параметри, так і величину вартості.

Вартість вважають нечіткою множиною, оскільки її залежність від показників якості або технічних параметрів рідко знаходить застосування в аналізі, відноситься до вузькоспеціалізованих систем і швидко старіє в часі. Проте перетворення нечіткої множини вартості у випадкові величини не є складним завданням, в результаті рішення якої можна отримати лінії середньоквадратичної регресії вартості на параметри, з якими модель ефективності системи адекватна і задача нелінійного програмування має, як правило,

оптимум. Задачі оптимізації можна вирішувати за умови широких обмежень, оскільки самі лінії середньоквадратичної регресії діапазонні, а їх застосування дозволяє отримати результат в аналітичному вигляді, що має швидку збіжність і універсальність програми оптимізації.

Оптимальне рішення задачі синтезу для оптоволоконної лінії зв'язку можна визначити методом математичного програмування, де рішення досягається при регулюванні кроків ітерації, число яких значно скорочується за рахунок використання оптимальних рішень типових задач. Так само можна знаходити оптимальне рішення за умовним критерієм якості, по вектору їх показників і вартості елементів реальних оптоволоконних систем, як мінімум у вигляді техніко-економічної статистики.

УДК 621.991(681)14

*М.О. Колісник
M.Kolisnyk*

**АНАЛІЗ МЕТОДІВ ЗАХИСТУ МЕРЕЖ INTRANET ВІД РІЗНОГО РОДУ
УРАЗЛИВОСТЕЙ**

**ANALYSIS METHODS TO PROTECT NETWORKS INTRANET FROM ALL SORTS OF
MALICIOUS ACTIONS**

В даний час на Укрзалізниці активно впроваджується мережа Intranet, яка передбачає використання робочих станцій та серверів баз даних, на які можуть мати вплив зловмисники.

До найбільш використовуваних зловмисниками впливів можна віднести використання вірусів, троянських коней, червей (Worms), IP-spoofing, Mac-flooding,

використання програмних закладок для реалізації Dos і DDos-атак, Brute-force атак, різноманітних ін'єкцій, програм-сніферів та ін.

Зважаючи на те, що на сервери баз даних різних підприємств все частіше здійснюються впливи зловмисників, актуальною задачею є аналіз існуючих методів захисту від різних видів уразливостей корпоративних мереж