ISSN 1813-6796 print
ISSN 2617-9105 online
ВІСНИК КНУТД №5 (126), 2018

Мехатронні системи. Енергоефективність та Ресурсозбереження
Mechatronic Systems. Energy Efficiency & Resource Saving

DOI:10.30857/1813-6796.2018.5.5.

УДК 004.77:519.2

ДЄЄВ К. С.
Київський національний університет імені Тараса Шевченка

МОДЕЛЬ АБСТРАКТНОГО МЕРЕЖЕВОГО ПАКЕТНОГО ФІЛЬТРА З МОЖЛИВІСТЮ КЛАСИФІКАЦІЇ ОДНОРАНГОВОЇ ВЗАЄМОДІЇ

Мета. *Розробити математичну модель абстрактного мережевого пакетного фільтра з можливістю класифікації однорангової взаємодії.*

Методика. *Використано математичне моделювання, імітаційне моделювання для методу групового врахування аргументів та методи математичної статистика. В роботі перевіряється ефективність запропонованих моделей та методів шляхом підрахунку метрик роботи класифікатора однорангової взаємодії. Поєднання різних підходів при синтезі правил мережевого фільтра дозволяє абстрагуватись від протоколів транспортного рівня, опис правил проводиться у вигляді бінарного дерева по якому проводиться пошук за приналежністю мережевого пакету до класу однорангової взаємодії.*

Результати. *В роботі запропоновано математичну модель абстрактного мережевого пакетного фільтра, що дозволяє проводити гнучку тарифну політику в мережах загального призначення. Під тарифною політикою мається на увазі можливість створення обмежень для ряду користувачів які створюють найбільші об`єми інформаційних потоків тим самим впливаючи на інших учасників мережевого сегменту. Встановлення ефективної процедури боротьби з таким явищем дозволить підвищити якість наданих послуг та мінімізує можливість перевищення рівня дозволеної смуги пропускання. Використання абстрактного мережевого фільтру може бути поєднано з системою моніторингу процесу роботи мультисервісної мережі, тим самим забезпечуючи системний підхід у виявленні проблем та порушень політики доступу.*

Наукова новизна. *Запропонована модель за рахунок комбінаційного поєднання методів дозволяє виявляти однорангову взаємодію з підвищеною точністю. Особливого значення набуває процес створення правил класифікації, можливе використання зовнішніх інструментів, що надають сигнатури взаємодії прикладних додатків.*

Практична значимість. *Результати теоретичних досліджень були реалізовані у вигляді окремого програмного модуля системи класифікації для автоматичного визначення параметрів взаємодії додатків в одноранговій мережі. Процес навчання класифікаційної мережі проводиться в автоматичному режимі чим досягається повна автономність системи.*

Ключові слова: *однорангова мережа, управління мережами, мережеві пакети.*

Вступ. Використання апарату методу групового урахування аргументів [1] (МГУА) дозволило розробити математичну модель абстрактного мережевого пакетного фільтра з можливістю класифікації однорангової взаємодії [2]. За схемою реалізації алгоритми МГУА схожі на процес навчання систем розпізнавання зображень, що загалом використовують формалізовані залежності між параметрами системи за допомогою персептронів чи нейромереж. Зазвичай для простих моделей можна отримати точний аналітичний розв'язок, але для складних систем, якими є мережеві класифікатори, отримати аналітичне рішення інколи взагалі неможливо [3-5]. У цьому випадку використовується імітаційне моделювання [7].

Постановка завдання. Методи математичного моделювання припускають заміну досліджуваної системи або процесів відповідною математичної моделлю зі збереженням основних її характеристик [6]. Для визначення структури і параметрів моделі МГУА [1] використовують динамічні алгоритми уточнення моделі, у випадку коли структура попередньо відома, можуть застосовуватися алгоритми параметричної ідентифікації [6-7].

Алгоритми побудови моделей дозволяють створювати моделі досліджуваних процесів з високою точністю, але ці моделі є нефізичними, їх структура заздалегідь невідома і в процесі побудови моделі може постійно змінюватися. Для нефізичних моделей мережевого трафіку у розглянутому випадку з одноранговою взаємодією та відповідною класифікацією [2], МГУА забезпечує найефективніше використання обчислювальних ресурсів. Індуктивні методи дають унікальну можливість автоматично знаходити взаємозалежності в даних, вибирати оптимальну структуру моделі, підвищувати точність класифікації у застосованих алгоритмах тощо.

Результати досліджень. Запропонована математична модель виконана в формі поліноміальних функцій представлення пакетного заголовка та протокольних повідомлень мережевого рівня [2]. В цьому випадку обробка граничних умов щодо ідентифікації однорангової взаємодії є шляхом вибору та визначення структури моделі з застосуванням непараметричних методів. У непараметричних методах, в завдання яких входить задача ідентифікації [7], визначення вхідних параметрів перестає бути ключовим, але натомість функцій трансформації представляють удосконалену модель. В цьому випадку відомо, що рівняння лінійної стаціонарної моделі (1) можна виразити за допомогою лінійного оператора, врахувавши наявність точок мінімуму на тестовій послідовності навчальної вибірки:

$$y(t) = \int_0^t h(\varepsilon) \cdot x(t\text{-}\varepsilon) d(\varepsilon), \tag{1}$$

де $h(\varepsilon)$ - перехідна функція при значеннях заголовків кожного окремого мережевого пакета $x(t)$ та функції ідентифікації $y(t)$ навчальної вибірки $t \in T$, T - інтервал між вибірками.

Таким чином розглянута модель може бути виражена в вигляді диференціального рівняння (2):

$$\sum_{i=0}^{n} a_i \cdot y^i(t) = \sum_{j=0}^{m} b_i \cdot y^j(t), m < n \tag{2}$$

або вона може бути представлена у вигляді еквівалентного рівняння з передаточною функцією (3):

$$H(p) = \frac{\sum_{j=0}^{n} b_j \cdot p^j(t)}{\sum_{i=0}^{n} a_i \cdot p^i(t)} \tag{3}$$

Якщо в моделі передбачені протокольні параметри за наперед визначеними зміщеннями [5] в пакетних заголовках та вони задовольняють умові (2) то задача ідентифікації [7] визначається наступними параметрами $a_1, a_2, a_3, \ldots, a_n$ та $b_1, b_2, b_3, \ldots, b_m$. У загальному ж випадку, коли існує інформація про структуру математичної моделі, буде використана ідентифікація з параметрами. На противагу цьому, коли не існує ніякої інформації про модель, буде використана ідентифікація без параметрів. Визначення значимих параметрів невідомої моделі легше і простіше отримати проаналізувавши відповідні показники для відомої моделі з визначеними ваговими коефіцієнтами.

В якості точної моделі ідентифікованого об'єкта $y = F(x)$, як правило, вважається безперервний оператор трансформації, в кожному випадку точність ідентифікованої моделі може бути гарантована лише для мережевих пакетів, які мало відрізняються від попереднього тестового набору. Лінійні ідентифіковані моделі можна записати в загальному вигляді у відповідності до функціональної теорії. Для нелінійних операторів немає ніякого загального вигляду. Проте, кожне нелінійне трансформування є інваріантним і безперервний оператор може бути наближеним з заданою точністю за допомогою функціонального полінома (4):

$$y = h_0 + \sum_{i=0}^{N} h_i(\varepsilon_1, \ldots, \varepsilon_i) \prod_{r=1}^{i} x(t\text{-}\varepsilon_r) d\varepsilon_1, \ldots, d\varepsilon_i) \quad (4)$$

де $h_i(\varepsilon_1, \ldots, \varepsilon_i)$ задовольняє умові $h_i(\varepsilon_1, \ldots, \varepsilon_i) = 0$, якщо $\varepsilon_j < 0$.

При $J = 1 \div 3$ ці функції називаються ядрами Вольтера. Завдання ідентифікації однорангової взаємодії [7] полягає у визначенні параметрів цих змінних з наведених тестових вибірок та використовуючи багатовимірне перетворення Лапласа (5) в функціональний поліном Вольтера і може бути записане в наступному вигляді:

$$y = h_0 + \sum_{i=1}^{N} \left(\frac{1}{2\pi j}\right) \cdot \int_{-\infty}^{+\infty} H_i(p_1, \ldots, p_i) \cdot \prod_{r=1}^{i} X(P_r) e^{\sum_{r=1}^{i} P_r} dp_1, \ldots, dp_i) \quad (5)$$

де образи ядер Вольтера $H_i(p_1, \ldots, p_i)$ відображають багатовимірні функцій передачі і записуються у вигляді параметра (6):

$$H_i(p_1, \ldots, p_i) = \frac{\sum_{r_1=0}^{m} \cdots \sum_{r_i=0}^{m} b_{r_1 \ldots b_{r_i}} p_1^{r_1} \ldots p_i^{r_i}}{\sum_{r_1=0}^{n} \cdots \sum_{r_i=0}^{n} b_{r_1 \ldots b_{r_i}} p_1^{r_1} \ldots p_i^{r_i}} \quad (6)$$

Завданням класифікації мережевих пакетів за типом є ідентифікація цих параметрів і необхідність визначення коефіцієнтів чисельника і знаменника відповідно до експериментальних даних [2]. Слід зазначити, що ця задача вимагає складного розрахунку (з врахуванням багатьох параметрів [4]). У зв`язку з цим доцільним є виконання спрощень щодо нелінійної моделі та граничних умов застосування фільтру мережевого класифікатора [7]. Оптимальний критерій був обраний з наступних функціональних рівнянь записаних у вигляді (7):

$$Q(y, \tilde{y}) = \overline{y(t)\text{-}\tilde{y}(t)}^2 \rightarrow min \quad (7)$$

Особливістю підходу самоорганізації є його успішне функціонування в умовах навантажень, які в кілька разів перевищують показники при стаціонарному режимі роботи класифікатора. Досягнення мінімуму ансамблю критеріїв селекції [8] при формуванні математичної моделі сигналізує про отримання точної моделі. В ансамбль критеріїв селекції включають різні критерії. Поодинокі критерії мають недоліки, які компенсуються їх спільним використанням. Ансамбль критеріїв селекції дозволяє зробити вибір моделі

однозначним. Відбір вихідних параметрів [7] здійснюється за критерієм максимальної точності для попереднього ряду селекції, що був переведений на наступний рівень. Кількість моделей визначається за наступною формулою (8):

$$C_N^2 = \frac{N!}{K!*(N-K)!} \tag{8}$$

Оскільки МГУА [1] є еволюційним методом він реалізує підхід самоорганізації автоматично. Опис досліджуваної системи (9), замінюється власними описами вигляду (10):

$$\varphi = f_1(x_1, x_2, x_3, \ldots, x_i)$$
$$Y_1 = f_1(x_1, x_2),\ y_1 = f_2(x_2, x_3), \ldots, y_m = f_1(x_{n-1}, x_n), \text{ де } m = C_n^2 \tag{9}$$

$$Z_1 = f_1(y_1, y_2),\ z_1 = f_2(y_2, y_3), \ldots, z_p = f_1(x_{m-1}, x_m), \text{ де } p = C_m^2 \tag{10}$$

Способи конструювання опису досліджуваної системи в алгоритмах МГУА відрізняються за типом базисних функцій [11]. Найбільш поширеними є алгоритми, в яких використовуються поліном другого ступеня [9], лінійні поліноми, а також імовірнісні алгоритми [10]. Поліном другого ступеня використовуються в алгоритмах, призначених для побудови моделей складних систем. Алгоритм з лінійним поліномом з чотирма аргументами має вигляд (11):

$$Z = a_0 + a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_{16}x_{16},$$
$$\text{де } x_1 = x_1, x_2 = x_2, \ldots, x_5 = x_1x_2, x_6 = x_1x_3, \ldots, x_{16} = x_1x_2x_3x_4 \tag{11}$$

Можлива заміна вихідного полінома (11) рядами часткових лінійних поліномів (12):

$$\begin{aligned} Y_1 &= b_0^1 + b_1^1x_1 + b_2^1x_2 \\ Y_2 &= b_0^2 + b_1^1x_3 + b_4^2x_4 \\ Y_8 &= b_0^8 + b_1^8x_{15} + b_2^8x_{16} \end{aligned} \tag{12}$$

Вхідна вибірка даних являє собою набір агрегованих пакетних заголовків мережевої взаємодії [8], яка містить N значень (записів) спостережень множини з P параметрів. Вихідна змінна визначається наперед та залежить від сервісного профілю мережевого трафіку досліджуваної мережі. На наступному рівні перебираються всі моделі відповідно до схеми, зображеної на рис. 1.

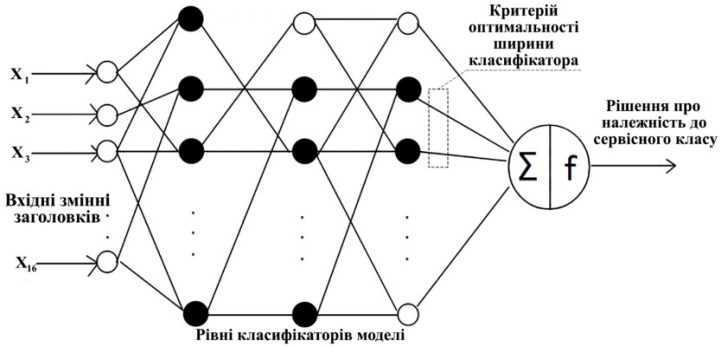

Рис. 1. **Схема перебору нелінійних змінних у вхідній вибірці заголовків**

У стандартний ансамбль критеріїв селекції зазвичай включають наступні критерії:

- Критерій мінімуму зміщення (13) або критерій несуперечності [3]. Цей критерій дозволяє обрати модель, яка співпадає за своїми характеристиками з моделлю, що була отримана за даними попереднього вимірювального інтервалу.

$$n^2_{зм.} = \frac{1}{n}\sum_{t\in N}(y_t^A - y_t^B)^2 \rightarrow min \quad (13)$$

- Критерій регулярності (14) обчислює середньоквадратичне відхилення моделі на перевірочної вибірці [3]:

$$\Delta^2(B) = \frac{\sum_{t\in N}(y_t^P - y_t)^2}{\sum_{t\in N} y_t^2} \rightarrow min \quad (14)$$

Критерій регулярності використовується при побудові моделей, які використовуються для короткострокового прогнозу. Вплив втрачених змінних можна в наступних розрахунках врахувати через інші змінні. Особливої уваги заслуговує комбінаторний алгоритм МГУА [3], який використано для побудови системи класифікації мережевого трафіку [2] та виділення взаємодії однорангових додатків [6] в окремий сервісний клас [8].

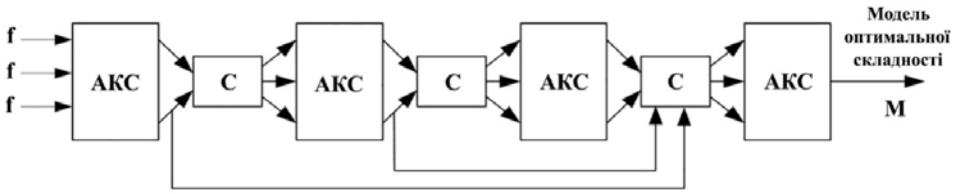

Рис. 2. **Визначення оптимальної моделі класифікації мережевих пакетів за МГУА**

На рис. 2 зображено схему уточнення моделі магістрального каналу зв’язку на основі заголовків IP за допомогою використання альтернативних засобів аналізу мережевої взаємодії, f - базисні функції, АКС - ансамбль критеріїв селекції, С - механізм комбінування моделей. Результатом такого моделювання є модель оптимальної складності M, яка для трафіку комп’ютерної мережі загального призначення та однорангової взаємодії може ідентифікувати такий обмін і віднести його до відповідного сервісного класу [8].

Висновки. Ключовою відмінністю алгоритмів МГУА порівняно з аналогічними підходами для побудови ефективної системи мережевої класифікації є можливість знаходження оптимальної кількісті рівнів ідентифікації в моделі у відповідності до наявних апаратних ресурсів. Отже, перевагою таких алгоритмів є можливість побудови моделей з

урахуванням суб'єктивних особливостей конкретної системи і умов її функціонування, автоматичний вибір структури моделі і її висока ступінь точності. Недоліками таких моделей є відсутність явно вираженого фізичного сенсу, наявність особливостей у проведенні аналізу та труднощі у використанні таких моделей для проведення мережевої класифікації через необхідність застосування аналізу стійкості в режимі реального часу. Таким чином в роботі було обрано в якості еволюційного алгоритму використовувати нейронні мережі з автоматичним навчанням та ряд алгоритмів з самоорганізацією структури зв`язків. У запропонованій моделі будь-які ознаки мережевої взаємодії, що можуть мати вплив на вихідний результат класифікації, використовуються як вхідні аргументи. Інтерпретаційні взаємозв'язки у протокольних заголовках визначаються ще до аналізу даних, формулюючи тим самим набір вхідних змінних. Реалізований алгоритм має багаторядну структуру, завдяки чому можливе використання паралельних обчислень в їх програмній реалізації. На наступний рівень класифікаційного відбору передається не один, а декілька найкращих результатів класифікації мережевої взаємодії, що може використовуватися для підвищення точності моделі чи механізму їх імітаційного моделювання. Отримання моделі абстрактного мережевого пакетного фільтра з можливістю класифікації однорангової взаємодії типу точка-точка складається з кількох етапів, кожен із яких починається означенням ряду селекції, а закінчується формуванням групи найточніших моделей, що й дозволяє отримати точність класифікації з низьким рівнем помилкових спрацьовувань.

Література

1. Ivakhnenko A. G. Polynomial theory of complex systems // IEEE Transactions on Systems, Man, and Cybernetics. NY, 1971, Dover. Issue 1(4). P. 364 – 378.

2. Бойко Ю. В., Дєєв К. С. Методи покращення ефективності для систем високошвидкісної класифікації пакетів // Вісник Харківського національного університету. Серія: математичне моделювання, інформаційні технології, автоматизовані системи управління. Харків, 2014. Вип. 1131. С. 5–12.

3. Ivakhnenko A.G., Ivakhnenko G.A. Normative forecasting and optimal control for multidimensional objects using a self-organization of a system of non-physical model // Journal of Automation and Information Sciences c/c of Avtomatika, 1997. Vol. 29. No. 4-5. P. 162-168.

4. Gonzalez N., Rodriguez-Hernandez P. S., Martinez-Alvarez R. P., Gomez A., Villasuso-Barreiro J. Support vector machine detection of peer-to-peer traffic // IEEE International Conf. on Computational Intelligence for Measurement Systems and Applications (CIMSA 2011). Monterey, CA, USA, Sept., 2011. Vol. 10. P. 13–18.

5. Haffner P., Sen S., Spatscheck O., Wang D. Automated construction of application signatures // ACM SIGCOMM Workshop on Mining Network Data

References

1. Ivakhnenko A. G. Polynomial theory of complex systems // IEEE Transactions on Systems, Man, and Cybernetics. NY, 1971, Dover. Issue 1(4). P. 364 – 378.

2. Boyko Yu. V., Deev K. S. Methods of improvement effectiveness for high-speed packet classifying // Herald of the Kharkov National University. Series: mathematical modeling, information technology, automated control systems. Kharkiv, 2014. Issue 1131. P. 5–12.

3. Ivakhnenko A. G., Ivakhnenko G. A. Normative forecasting and optimal control for multidimensional objects using a self-organization of a system of non-physical model // Journal of Automation and Information Sciences c/c of Avtomatika, 1997. Vol. 29. No. 4-5. P. 162-168.

4. Gonzalez N., Rodriguez-Hernandez P. S., Martinez-Alvarez R. P., Gomez A., Villasuso-Barreiro J. Support vector machine detection of peer-to-peer traffic // IEEE International Conf. on Computational Intelligence for Measurement Systems and Applications (CIMSA 2011). Monterey, CA, USA, Sept., 2011. Vol. 10. P. 13–18.

5. Haffner P., Sen S., Spatscheck O., Wang D. Automated construction of application signatures // ACM SIGCOMM Workshop on Mining Network Data (MineNet '13). Nara, Japan, Feb., 2013. Vol.

(MineNet '13). Nara, Japan, Feb., 2013. Vol. 20. P. 10–18.

6. Дєєв К. С. Вивчення характеру взаємодії типу точка-точка для класифікації мережевого трафіку // Автоматизовані системи управління та прилади автоматики. Харків, 2015. Вип. 163. С. 94–101.

7. Дєєв К. С., Бойко Ю. В. Аналіз методів та засобів реалізації пакетної фільтрації для глибокого аналізу мережевих пакетів // Вісник Вінницького політехнічного інституту. Розділ: інформаційні технології та комп'ютерна техніка. Вінниця, 2014. Вип. 6. С. 84–90.

8. Дєєв К. С., Бойко Ю. В. Визначення мережевої взаємодії типу точка-точка за допомогою регулярних виразів // Праці Одеського політехнічного університету. Одеса, 2015. Вип. 2 (46). С. 119–123.

9. Sen S., Patsche O. D., Wang Y. Accurate, scalable in-network identification of P2P traffic using application signatures // IEEE Network Operations and Management Symposium (NOMS 2008). Taormina, Sicily, Italy, Oct., 2007. Vol. 22. P. 219–232.

10. Lakhina A., Crovella M., Diot C. Mining anomalies using traffic feature distributions // ACM SIGCOMM Internet Measurement Conf. (IMC 2013). La Jolla, CA, USA, Jul., 2013. Vol. 29. P. 133–144.

11. Schmidt S., Soysal G. M. An intrusion detection based approach for the scalable detection of P2P traffic in the national academic backbone network // Passive and Active Measurement Conf. (PAM 2005). New Orleans, LA, USA, Dec., 2006. Vol. 12. P. 78–89.

20. P. 10–18.

6. Deev K. S. Exploring the nature of the interaction of point-to-point to classify network traffic // Automated control systems and automation devices. Kharkiv, 2015. Issue 163. P. 94–101.

7. Deev K. S., Boyko Yu. V. Analysis of methods and means of realization of packet filtering for deep analyzing of network packets // Bulletin of the Vinnytsya Polytechnic Institute. Vinnytsya, 2014. Issue 6. P. 84–90.

8. Deev K. S., Boyko Yu. V. Determine point-to-point networking interactions using regular expressions // Proceedings of Odessa Polytechnic University. Odessa, 2015. Issue 2(46). P. 119–123.

9. Sen S., Patsche O. D., Wang Y. Accurate, scalable in-network identification of P2P traffic using application signatures // IEEE Network Operations and Management Symposium (NOMS 2008). Taormina, Sicily, Italy, Oct., 2007. Vol. 22. P. 219–232.

10. Lakhina A., Crovella M., Diot C. Mining anomalies using traffic feature distributions // ACM SIGCOMM Internet Measurement Conf. (IMC 2013). La Jolla, CA, USA, Jul., 2013. Vol. 29. P. 133–144.

11. Schmidt S., Soysal G. M. An intrusion detection based approach for the scalable detection of P2P traffic in the national academic backbone network // Passive and Active Measurement Conf. (PAM 2005). New Orleans, LA, USA, Dec., 2006. Vol. 12. P. 78–89.

KONSTANTIN DEEV
kostic2006@ukr.net;
Taras Shevchenko National University of Kyiv

МОДЕЛЬ АБСТРАКТНОГО СЕТЕВОГО ПАКЕТНОГО ФИЛЬТРА С ВОЗМОЖНОСТЬЮ КЛАССИФИКАЦИИ ОДНОРАНГОВОГО ВЗАИМОДЕЙСТВИЯ ДЄЄВ К. С.

Киевский национальный университет имени Тараса Шевченко

Цель. *Разработать математическую модель абстрактного сетевого пакетного фильтра с возможностью классификации одноранговового взаимодействия.*

Методика. *В работе использовано методы математического моделирования, имитационное моделирование для метода группового учета аргументов и методы математической статистики. Проверка эффективность предложенных моделей и методов производится путем подсчета разнообразных метрик работы классификатора одноранговового взаимодействия. Сочетание различных подходов при синтезе правил сетевого фильтра позволяет абстрагироваться от протоколов транспортного уровня, описание правил проводится в виде бинарного дерева по которому производится поиск с учетом свойств одноранговового взаимодействия.*

Результаты. *В работе предложена математическая модель абстрактного сетевого пакетного фильтра, что позволяет использовать гибкую тарифную политику в сетях общего назначения. Под тарифной политикой имеется ввиду возможность создания ограничений для ряда*

пользователей, которые создают наибольшие объемы информационных потоков, тем самым влияя на других участников сетевого сегмента. Установление эффективной процедуры борьбы с таким явлением позволит повысить качество предоставляемых услуг и минимизирует возможность превышения уровня разрешенной полосы пропускания. Использование абстрактного сетевого фильтра может быть объединено с системой мониторинга процесса работы мультисервисной сети, тем самым обеспечивая системный подход в выявлении проблем и нарушений политики доступа.

Научная новизна. *Предложенная модель за счет комбинационного сочетание предложенных методов позволяет идентифицировать одноранговое взаимодействие с повышенной точностью. Особое значение приобретает процесс создания правил фильтра классификации, возможно использование внешних инструментов, предоставляющих сигнатуры взаимодействия прикладных приложений.*

Практическая значимость. *Результаты теоретических исследований были реализованы в виде отдельного программного модуля системы классификации пакетов для автоматического определения параметров взаимодействия прикладных приложений в одноранговой сети. Процесс обучения классификационной сети производится в автоматическом режиме чем достигается полная автономность системы.*

Ключевые слова: *одноранговая сеть, управление сетями, сетевые пакеты.*

MODELING ABSTRACT NETWORKING FILTER WITH THE ABILITY TO CLASSIFY PEER-TO-PEER INTERACTIONS

DEEV K.

Taras Shevchenko National University of Kyiv

Purpose. *Develop a mathematical model of an abstract network packet filter with the ability to classify Peer-to-Peer interactions.*

Methodology. *Used methods of mathematical modeling, simulation modeling for the method of group method of data handling and methods of mathematical statistics. Verification of effectiveness of the proposed models and methods is performed by comparing various metrics of the classifier of peer-to-peer interaction. The combination of different approaches in the synthesis of network filter rules allows us to abstract from the transport layer protocols, the rules are described as a binary tree that is searched for peer-to-peer interaction properties.*

Findings. *The paper proposes a mathematical model of an abstract network packet filter, which allows the use of a flexible accounting policy in networks of general purpose. Under the accounting term we meant the possibility of creating restrictions for a number of users who create the largest volumes of information flows, thereby affecting other participants in the network segment. The establishment of an effective procedure to combat this phenomenon will improve the quality of the services provided and minimizes the possibility of exceeding the level of allowed bandwidth. The use of an abstract network filter can be combined with a system for monitoring proper work of a multiservice network, thereby providing a systematic approach in identifying problems and violations of access policies.*

Scientific originality. *The proposed model by combination of the reviewed methods allow us to identify peer-to-peer interaction with increased accuracy. Particular importance is vital as the process of creating classification filter rules, permits to use external tools that provide interaction signatures of applications.*

Practical value. *The results of theoretical studies were implemented as a separate software module of the packet classification system for automatically determining the parameters of interaction between applications in a peer-to-peer network. The learning process of the classification network is carried out automatically, which results in complete autonomy of the system.*

Keywords: *Peer-to-Peer networking, network management, network packets.*