УДК 621.391 160164

С.М. ЛИСЕНКО, К.Ю. БОБРОВНІКОВА, В.І. ДМИТРУК, А.С. АДАМЕНКО
Хмельницький національний університет

МЕТОД ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ КОМП'ЮТЕРНИХ СИСТЕМ В КОРПОРАТИВНИХ МЕРЕЖАХ НА ОСНОВІ САМОАДАПТИВНОСТІ

В роботі представлено метод забезпечення живучості комп'ютерних систем в корпоративних мережах на основі самоадаптивності. Метод дозволяє забезпечити живучість комп'ютерних систем в корпоративних мережах шляхом адаптивного переналаштування конфігурації мережі та параметрів комп'ютерних систем. Метод базується на кластерному аналізі ознак, отриманих шляхом дослідження появи кібер-загроз щодо комп'ютерних систем в корпоративних мережах.

Ключові слова: адаптивні системи, самоадаптивність, резильєнтність, кібер-загроза, кібер-атака, шкідливе програмне забезпечення, DDoS-атака, фішинг.

S. LYSENKO, K. BOBROVNIKOVA, V. DMYTRUK, A. ADAMENKO
Khmelnytskyi National University

TECHNIQUE FOR COMPUTER SYSTEMS RESILIENCE IN THE CORPORATE AREA NETWORKS BASED ON THE SELFADAPTIVITY

The paper presents a technique for computer systems resilience in the corporate area networks based on the selfadaptivity. It allows the persisting of the computer systems resilience in networks by adaptive based on the reconfiguring of the network configuration and computer systems parameters. The method is based on cluster analysis using the features obtained by analysis of the of cyber threats concerning to the computer systems in corporate area networks. An approach employs the semi-supervised fuzzy c-means clustering. Use of the developed method makes it possible to keep the computer systems functioning in the situation of cyber –attacks.

Keywords: computer systems, adaptive systems, selfadaptivity, resilience, cyber threat, attack, malware, DDoS attack, fishing.

Вступ. На сьогоднішній день кібер-загрози є однією з найбільш небезпечним явищем в інформаційному світі [1], а також одним з основних можливостей нелегального заробітку в мережі Інтернет. Відомими кібер-загрозами є DDoS атаки (розподілені атаки типу «відмова в обслуговуванні»), атаки для здійснення збору та викрадення конфіденційної інформації користувачів, розсилання спаму з шкідливим програмним забезпеченням (ШПЗ), застосування засобів нав'язування реклами, фішинг, накрутка клік-лічильників (клікфрод), створення пошукового спаму, використання інфікованих комп'ютерів для зберігання нелегального матеріалу (піратське ПЗ, порнографія тощо) та в якості проксі-серверів для анонімізації доступу в мережі Інтернет. Щороку по всьому світу кібер-атакам піддаються близько 800 млн комп'ютерних систем (КС), щосекунди – близько 60 ПК. За попередній рік кібер-атаки нанесли збитків світовій економіці в $110 млрд [2].

Відомі методи боротьби з кібер-атаками демонструють їх недостатню ефективність, оскільки у випадку успішної атаки збоку зловмисника не вирішують проблему подальшого нормального функціонування комп'ютерної системи в корпоративній мережі, тобто не забезпечують її живучість (резильєнтність).

Тому постає актуальна науково-практична задача розробки методу забезпечення живучості (резильєнтності) комп'ютерних систем в корпоративних мережах на основі самоадаптивності.

Самоадаптині системи як засоби резильєнтності комп'ютерних систем в умовах здійснення кібер-атак. Поява нових кібер-загороз, збільшення кількості шкідливого програмного забезпечення вимагає нових інноваційних підходів до забезпечення інформаційної безпеки комп'ютерних систем в корпоративних мережах [3]. Наслідком безперервної еволюції кібер-загроз, системи інформаційної безпеки повинні ставати більш універсальними, гнучкими та самоадаптивними, а саме такими, що здатні до самопереконфігурації в залежності до зміни експлуатаційних контекстів і умов. Велика кількість умов, що впливають на нормальне функціонування КС з точки зору їх захисту та забезпечення живучості у випадку здійснення кібер-атак, вимагає пошуку нових методів, які б мали здатність системи здійснювати налаштовування її поведінки у відповідь на його атаки.

Одним з найперспективніших напрямків, що вирішують проблеми забезпечення живучості (резильєнтності) є самоадаптивні системи [4].

Адаптивні системи в процесі функціонування здатні накопичувати інформацію з метою здійснення оцінки змін зовнішніх та/або внутрішніх умов та пристосовуватись до цих змін шляхом пасивної або активної адаптації власної поведінки. Пасивна адаптація передбачає реагування адаптивної системи на зміну умов шляхом оптимальної зміни її внутрішнього стану, активна адаптація полягає у здійсненні системою впливу на зовнішні умови з метою оптимальної зміни цих умов. Адаптація систем, що самоналаштовуються, досягається за рахунок зміни параметрів системи. Адаптивні системи, що самоорганізуються, пристосовуються до зміни зовнішніх умов шляхом зміни власної структури (організації). Метою адаптації може бути покращення функціональності, ефективності роботи системи та забезпечення її живучості в умовах повної або часткової невизначеності факторів, які можуть здійснювати

вплив на адаптивну систему [5].

Метод забезпечення живучості комп'ютерних систем в корпоративних мережах на основі само адаптивності. Запропоновано метод забезпечення живучості комп'ютерних систем в корпоративних мережах на основі самоадаптивності. Метод дозволяє забезпечити живучість комп'ютерних систем в корпоративних мережах шляхом адаптивного переналаштування конфігурації мережі та параметрів КС. Метод базується на кластерному аналізі ознак, отриманих шляхом дослідження появи потенційних кібер-загроз щодо комп'ютерних систем в корпоративних мережах.

Запропонований метод використовує нечітку кластеризацію с-середніх з частковим навчанням. Використання нечіткої кластеризації дозволяє отримати вищу точність та змістовність результату кластеризації в умовах інформаційної невизначеності [6].

Об'єктами кластеризації є вектори ознак, побудовані на основі відслідковування подій, що можуть вказувати на появи кібер-загрози, як комп'ютерних системах, так і в корпоративній мережі.

Метою методу є генерація сценаріїв поведінки комп'ютерних систем в мережі в умовах кібер-атак.

Метод складається з наступних кроків (рис.1):

1) збір вхідного мережного трафіка;

2) аналіз результатів роботи антивірусних засобів комп'ютерних систем;

3) побудова вектора ознак, вилучених з вхідного трафіка та звітів антивірусних засобів;

4) здійснення нечіткої кластеризації з частковим навчанням. Метою є кластеризації продукування результуючого сценарію, який адаптивно здійснює переналаштування сумісно множини параметрів щодо КС та мережі та дозволить продовження функціонування КС, а саме забезпечить її резильєнтність;

5) застосування вказівок щодо сценарію.

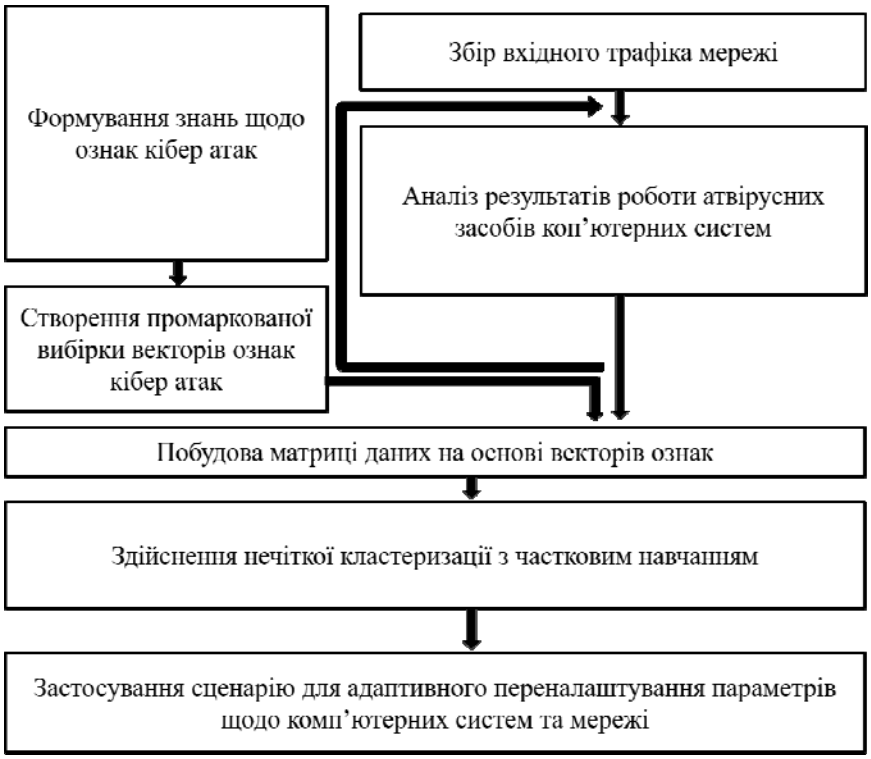


Рис. 1. Схема функціонування запропонованого методу

Формування знань щодо ознак, отриманих з вхідного мережного трафіка та з комп'ютерних систем в мережі.

З метою виявлення кібер-атак мережного типу здійснюється моніторинг активності мережі, і виконується постійний запис усіх параметрів, що можуть вказувати на появу кібер-атаки.

З боку комп'ютерних систем здійснюється постійне відслідковування системних подій, активності процесора, активності системних процесів та ін. Також виконується аналіз звітів антивірусних засобів комп'ютерних систем.

Таким чином, зібрану інформацію можна подати як вектор ознак, що вказуватиме на природу можливої кібер-загрози щодо КС:

$$\overline{W_{d\ i}} = \left(t, o_V, o_T, o_W, o_B, o_{LB}, o_S, o_M, o_R, a_{\exp}, a_{buf}, a_{DoS}, a_{pf}, a_s, a_{ps}, a_{mm}, a_{SQL}, a_{XSS}, a_{ph}, a_{DNSsp}, a_{IPsp}\right), \quad (1)$$

де t – тип КС;

o_V – поява ШПЗ типу вірус;

o_T – поява ШПЗ типу троянська програма;

o_W – поява ШПЗ типу worm-вірус;

o_B – поява ШПЗ типу в Backdoors;

o_{LB} – поява ШПЗ типу Logic Bombs;

o_S – поява ШПЗ типу Spyware;

o_M – поява ШПЗ типу Mailbombing;

o_R – поява ШПЗ типу Rootkit;

a_{exp} – exploit-атака;

a_{buf} – атака типу buffer overflows;

a_{DoS} – поява Denial-of-Service атаки щодо КС;

a_{pf} – ping flooding атака;

a_s – smurf атака;

a_{ps} - ping sweep атака;

a_{mm} - man-in-the-middle атака;

a_{SQL} – SQL/PHP-ін'єкції без відома адміністратора ресурсу;

a_{XSS} - XSS-атака;

a_{ph} - Phishing-атаки

a_{DNSsp} – DNS spoofing атака;

a_{IPsp} – IP spoofing атака.

Знання формуються на основі ознак властивих відомим кібер-загрозам, а також підозрілою поведінкою трафіка в мережі та програмного забезпечення в комп'ютерній системі:

$$if\ ((T_{ins})\ and\ (IP_{ins} \in A)) or ((T_{out})\ and\ (IP_{out} \notin A)) \Rightarrow sc_1,$$

де T_{ins}, T_{out} – вхідний та вихідний трафік відповідно;

IP_{ins}, IP_{out} – IP-адреси джерел вхідного та вихідного трафіка відповідно;

A – множина IP-адрес локальної мережі;

cs_1 – множина дій по відсіканню вхідного/вихідного трафіка.

$if\ (T_{type} = \text{type})\ and\ (T_{vol} > \lim_{\text{type}}) \Rightarrow sc_2$, де

T_{type} – тип трафіка;

T_{vol} – обсяг трафіка;

$\lim_{\text{type}}$ – припустимі межі обсягу для даного типу трафіка;

cs_2 – множина дій по обмеженню обсягу потенційно шкідливого трафіка.

$$if\ \left(t_{\text{mod}} \in [0,900]\ and\ t_{med} \in [0,900]\ and\ t_{aver} \in [0,900]\ \right)\ and$$

$$if\ \left(\left(n_A \in (5,\infty)\ and\ s_A \in (65535,\infty)\right) or \left(n_{UA} \in (8,\infty)\ and\ s_{UA} \in (65535,\infty)\right)\right) \Rightarrow sc2$$

$$if\ t_{\text{mod}} \in [0,900]\ and\ t_{med} \in [0,900]\ and\ t_{aver} \in [0,900]\ and$$

$$and\ f_S = 0\ and\ n_D \in [8;\infty] \Rightarrow sc3$$

$$if\ t_{\text{mod}} \in [0,900]\ and\ t_{med} \in [0,900]\ and\ t_{aver} \in [0,900]\ and$$

$$and\ n_{IP} \in (5,\infty)\ and\ s_{IP} \in (65535,\infty) \Rightarrow sc4$$

$$if\ \left(\left(l_N \in [75,255]\ and\ n_U \in (27,37]\right)\ or\ \left(e_N \geq f_{E_{B32}}\ or\right.\right.$$

$$\left.\left.or\ \left(e_R \geq f_{E_{B64}}\ or\ e_R \geq f_{E_{B256}}\right)\ or\ f_{UR} = 1\right)\right) and\ l_P > 300\ \Rightarrow sc5 \qquad (2).$$

$sc5$ - множина дій по локалізації та блокуванню ШПЗ типу бот.

Створення промаркованої вибірки векторів ознак кібер-загроз на основі знань.

Вибірка формується на основі знань щодо ознак кібер-загроз. На основі наявної вибірки здійснюється часткове навчання кластеризатора. Також на базі знань також створюється промаркована навчальна вибірка векторів ознак кіберзагроз. Приймемо промарковану вибірку даних як $X = \{x_i\}_{i=1}^{N_x}$, тоді немаркована вибірка позначиться як $Y = \{y_i\}_{i=1+N_x}^{N_z}$, де N_x – кількість об'єктів в промаркованій вибірці даних, N_z - загальна кількість об'єктів.

Приймемо $H = \{h_i\}_{i=1}^{N_h}$ – множина наперед визначених кластерів об'єктів, де N_h – кількість кластерів, належність вектора ознак кластеру h_1 свідчить про застосування одного з можливих сценаріїв переконфігурації параметрів мережі і/або комп'ютерної системи. Кожен вектор ознак з промаркованої вибірки даних належить одному з множини наперед визначених кластерів.

З векторів ознак атаки формується матриця даних V, кожен рядок якої є вектором ознак атак $\overline{W_d}$ щодо певної КС в мережі, $V = \left(v_{ij}\right)_{i=1,j=1}^{N_z,N_q}$, $V(i,) = \overline{W_d}$, де N_q – загальна кількість ознак, які вказують на здійснення атаки щодо КС в мережі.

Здійснення нечіткої кластеризації з частковим навчанням з метою генерації сценарію переналаштування параметрів мережі та КС.

На даному етапі здійснюється нечітка кластеризація векторів ознак атаки щодо КС з частковим навчанням на основі промаркованої навчальної вибірки. Задача кластеризації з частковим навчанням може опишемо функцією $f_{cluster} : W \to H$.

Результатом кластеризації є ступені приналежності векторів ознак до h кластерів $H = \{h_i\}_{i=1}^{N_h}$, де належність вектора ознак $\overline{W}$ кластеру h_i, свідчить про обраний сценарій здійснення адаптивного переналаштування параметрів мережі та КС в залежності від типу атаки. В якості відстані між об'єктом кластеризації та центром кластера в роботі було застосовано норму Махаланобіса.

Застосувння сценаріїв. На основі приналежності певного вектора ознак атаки до певного кластера здійснюється застосування сценарію, що містить інформацію щодо адаптивного переналаштування параметрів мережі та КС залежно від типу атаки. З цією метою виконується розсилання інформації про атаку, а також вказівки КС мережі.

Експерименти. Для визначення ефективності роботи запропонованого методу було проведено ряд експериментів. З цією метою було згенеровано тестове програмного забезпечення, що емулювало ряд кібер-атак щодо комп'ютерних систем в мережі. Дане програмне забезпечення було застосовано на КС локальної мережі, а також було використано ззовні по відношенню до вказаної мережі. Для експериментів була використана локальна мережа з 50 комп'ютерних систем. Експеримент тривав 24 години. Для проведення експериментів в якості навчальної вибірки було промарковано 10% векторів ознак щодо атак.

На рис. 2 відображено навчальну вибірку у вигляді проекції на площину множини векторів ознак атак, розподілених на результуючі кластери. Кожен маркер в кластері представляє атаку щодо КС мережі.

Результати роботи методу представлені на рис. 3, де продемонстровано прийняття рішення щодо певних атак.

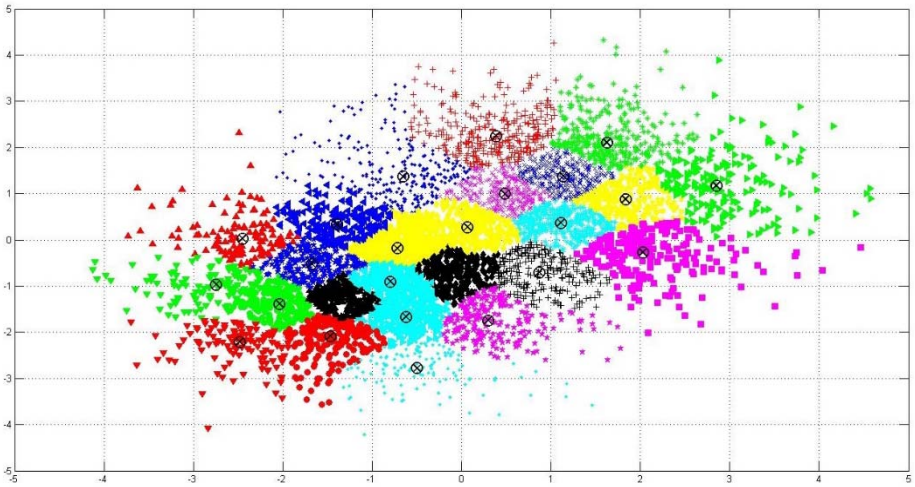
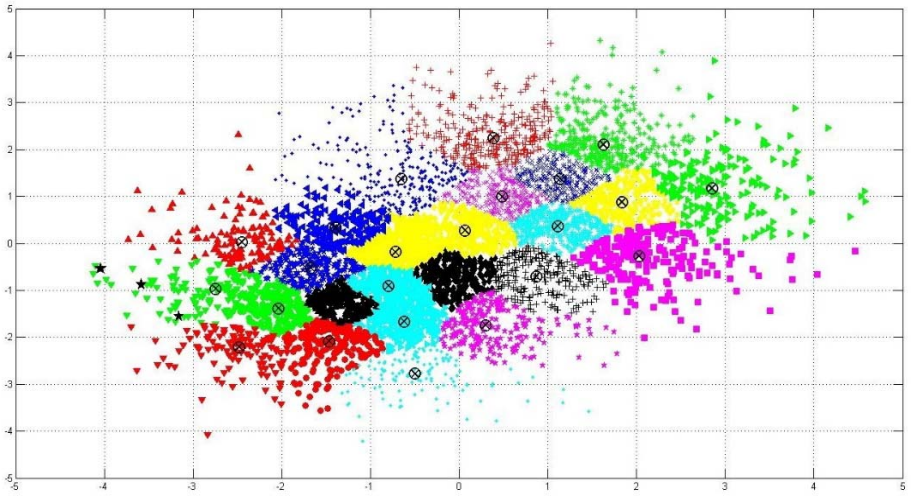
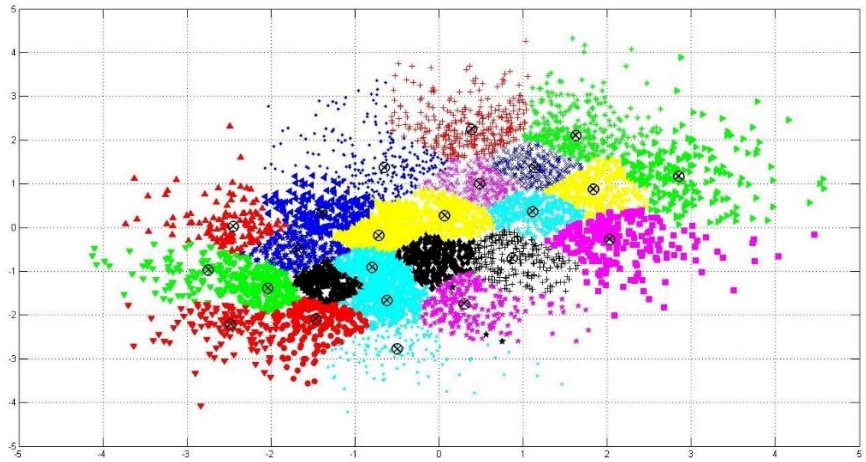


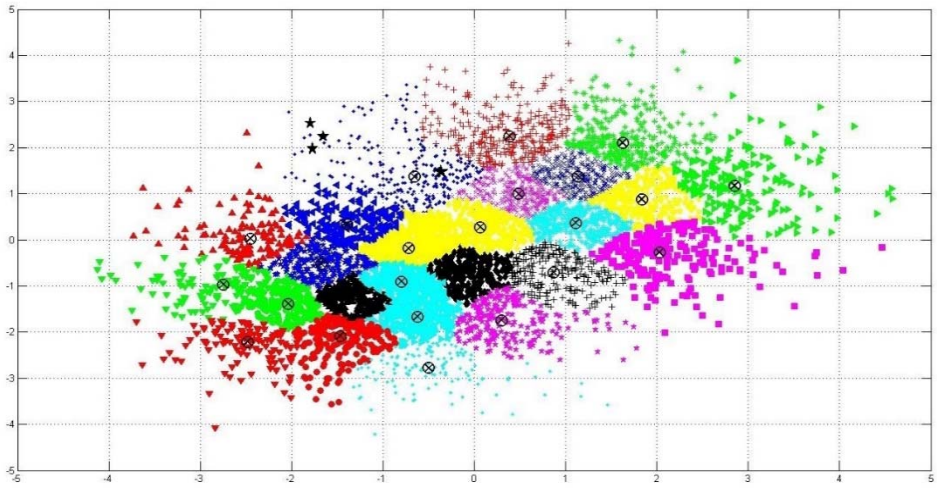
Рис. 2. Навчальна вибірка у вигляді проекції на площину множини векторів ознак атак, розподілених на результуючі кластери



а)



б)



в)

Рис. 3. **Результати кластеризації (маркери у вигляді зірок):**
а) для smurf атаки; б) для ping flooding атаки; в) ping sweep атаки

Таким чином залучення методу демонструє здатність забезпечення резильєнтності комп'ютерних систем в умовах кібератак шляхом залучення адаптивних підходів до їх захисту.

Висновки. Запропоновано метод забезпечення живучості комп'ютерних систем в корпоративних мережах на основі самоадаптивності. Метод дозволяє забезпечити живучість комп'ютерних систем в корпоративних мережах шляхом адаптивного переналаштування конфігурації мережі та параметрів комп'ютерних систем. Метод базується на кластерному аналізі ознак, отриманих шляхом дослідження появи потенційних кібер-загроз щодо комп'ютерних систем в корпоративних мережах.

Запропонований метод використовує нечітку кластеризацію с-середніх з частковим навчанням. Використання нечіткої кластеризації дозволяє отримати вищу точність та змістовність результату

кластеризації в умовах інформаційної невизначеності.

Література

1. Sochor, T., Zuzcak, M., Bujok, P. Analysis of attackers against windows emulating honeypots in various types of networks and regions. In: International Conference on Ubiquitous and Future Networks, 2016, pp. 863-868.

2. Tom C. W. Lin Financial Weapons of War Minnesota Law Review, Vol. 100, p. 1377, 2016 Temple University Legal Studies Research Paper No. 2016.

3. Kizza Joseph Migga Computer Network Security. Springer. ISBN: 0-387-20473-3.

4. Betty H.C. Cheng, Rog´erio de Lemos, Holger Giese, Paola Inverardi, Jeff Magee Software Engineering for Self-Adaptive Systems: A Research Roadmap. International Journal of Software Engineering & Applications (IJSEA), Vol.6, No.4, 2015.

5. Macías-Escrivá F. D. et al. Self-adaptive systems: A survey of current approaches, research challenges and applications. Expert Systems with Applications. – 2013. – Т. 40. – №. 18. – С. 7267-7279.

6. A comparison of distance-based semi-supervised fuzzy c-means clustering algorithms. Lai, D.T.C., Garibaldi, J.M.: Fuzzy Systems (FUZZ), In 2011 IEEE International Conference, 2011. – pp. 1580-1586.

Отримана/Received : 21.5.2017 р. Надрукована/Printed :10.6.2017 р.
Рецензент: д.т.н., проф.. Боровик В.В.

УДК 004.942:378.147

К.М. ЯЛОВА, К.В. ЯШИНА
Дніпровський державний технічний університет, м. Кам'янське

УНІВЕРСАЛЬНА ФУНКЦІОНАЛЬНА МОДЕЛЬ АКАДЕМІЧНОЇ MASSIVE OPEN ON-LINE COURSE ПЛАТФОРМИ

В роботі представлено результати побудови універсальної функціональної моделі академічної Massive open on-line course платформи. Запропонований графічний опис розробленої моделі надає наочне представлення про діючі особи предметної області, їх функції та схеми обміну інформацією. Наведена математична модель описує предметну область у формалізованому вигляді, що дозволяє більш поглиблено вивчати процеси внутрішнього трансферу знань у системі «студент-викладач». Виявлені функціональні залежності дозволяють перейти до логічного та фізичного проектування бази даних платформи та її програмної реалізації.

Ключові слова: дистанційне електронне навчання, функціональна модель, МООС-платформа, внутрішній трансфер знань

K. YALOVA, K. YASHYNA
Dnipro State Technical University, Ukraine

UNIVERSAL FUNCTIONAL MODEL OF THE ACADEMIC MASSIVE OPEN ONLINE COURSE PLATFORM

The main aim of the article is to provide results of the data domain analysis by the means of the academic massive open on-line course platform universal functional model as effective distance e-learning tools. In the article the results of the academic massive open on-line course platform universal function model creation are provided. Authors have developed the universal functional model on the base of the functional requirements and results of the comparative analysis of the modern distance and e-learning systems. The offered graphic representation of the developed model provides the visual description of data domain actors, their functions and information exchange diagrams. The using of the created functional model has allowed developing of the academic massive open on-line course platform architecture. The revealed functional dependencies are given the possibilities for modelling of the logical and physical platform database and its software. The given mathematical model describes data domain in the formalized form which allows studying more profoundly processes of an internal knowledge transfer in the «student-teacher» system.

Keywords: distance and e-learning, functional model, MOOC-platform, internal knowledge transfer.

Вступ

Швидкий розвиток інформаційних технологій (ІТ) дозволяє використовувати комп'ютерну техніку не тільки для обробки, зберігання або передачі інформаційних ресурсів (ІР), але також в якості засобу організації навчального середовища [1]. Розвиток технологій дистанційного навчання пройшов стадії від розповсюдження навчальних матеріалів через електронну пошту, системи електронного дистанційного навчання (ЕДН) на кшталт Modular Object-Oriented Dynamic Learning Environment (MOODLE) до масивних відкритих платформ он-лайн курсів - Massive open on-line courses (МООС). Серед яких слід відзначити EDX Гарвардського університету (США). МООС – це навчальний курс із масовою кількістю інтерактивних користувачів, які використовують технології електронного навчання та відкритого доступу до знань через Інтернет. У загальному розумінні академічна МООС-платформа – це система, що створена засобами інформаційних та цифрових технологій і забезпечує процес набуття знань, коли джерело інформації та студенти відокремлені часом та відстанню один від одного [2]. Слово «академічна» в даному визначенні відноситься до обов'язкового правила відповідності навчальних матеріалів платформи до встановлених нормативних документів певного університету, з певного напряму підготовки чи