УДК 004.056.53 : 004.492.3

Комар М.П.
Тернопільський національний економічний університет

Еволюція детекторів атак на інформаційні телекомунікаційні мережі в складі системи колективного інтелекту

Запропоновано використати засоби колективного інтелекту для виявлення та класифікації атак на інформаційні телекомунікаційні мережі. Розглянуто підхід до еволюції агентів (детекторів комп'ютерних атак), який базується на їх інтеграції у штучну імунну систему. В якості детектора атак запропоновано використати нейромережевий детектор, в основі якого лежить нейронна мережа LVQ, що дозволяє оперативно генерувати різноманітні детектори атак різних типів. При цьому застосовано базові принципи функціонування штучної імунної системи.

Ключові слова: колективний інтелект, мультиагентні системи, штучні нейронні мережі, штучні імунні системи, комп'ютерні атаки, виявлення та класифікація атак, нейромережевий імунний детектор.

Komar Myroslav
Ternopil National Economic University

The Evolution of Attacks Detectors on Information and Telecommunication Networks within the Collective Intelligence System

Collective intelligence tools for detection and classification of attacks on information and telecommunication networks are suggested. The approach to evolution of agents (detectors of computer attacks) based on the integration of artificial immune system is considered. Neural network is used as detector of attack. They are based on the LVQ neural network, that can quickly generate various detectors for different types of attacks. Basic principles operation of an artificial immune system are used at this approach.

Keywords: collective intelligence, multi-agent system, artificial neural networks, artificial immune systems, cyber attacks, detection and classification of attacks, immune neural network detector.

ВСТУП

В останній час значний розвиток отримали дослідження в області колективного (ройового) інтелекту (Swarm Intelligence) [1]. Даний науковий напрям виник в рамках напряму штучного інтелекту і описує колективну поведінку децентралізованої самоорганізованої адаптивної системи. Системи колективного інтелекту – це мультиагентні системи, які складаються з множини агентів, які взаємодіють між собою і з навколишнім середовищем, утворюючи таким чином колективний інтелект. В основу систем колективного інтелекту покладені біологічні основи поведінки тварин і на основі спостережень доведено, що груповий інтелект часто перевершує розумові здібності однієї особини.

На відміну від класичного підходу штучного інтелекту, за яким для певної задачі створюється одна інтелектуальна система, автором запропоновано використати мультиагентний підхід для виявлення та класифікації атак на інформаційні телекомунікаційні мережі (ІТМ), де один агент має неповне уявлення про глобальну загрозу, тому створюється множина агентів (детекторів атак) і забезпечується ефективна взаємодія між ними. Глобальна поведінка всієї системи розглядається, як результат взаємодії множини простих агентів.

В даній роботі в якості агента (детектора атак) запропоновано використати архітектуру нейронної мережі [2, 3], яка розроблена в [4, 5]. Запропоновано підхід до організації еволюції детекторів комп'ютерних атак на основі інтеграції нейромережевих детекторів в штучну імунну систему [6]. Реалізація даного підходу здійснюється на основі базових принципів і механізмів біологічної імунної системи: генерація і навчання імунних детекторів, відбір детекторів, які з певних причин генерують помилкові рішення, функціонування детекторів, активація детекторів і формування імунної пам'яті і на основі типової схеми штучної імунної системи, запропонованих в [6].

Нейромережеві імунні детектори (НІД) генеруються по випадковому алгоритму, що дає можливість створення великої кількості різноманітних за своєю структурою детекторів, які здатні реагувати на будь-яку аномалію. Потім, детектори проходять стадію навчання, на якій вони набувають здатності коректно реагувати на чужорідні об'єкти або явища. Для того, щоб детектори не генерували помилкові спрацьовування, вони ретельно відбираються. Ті з них, які не навчилися коректно класифікувати об'єкти – знищуються. Відібрані детектори допускаються до виконання функцій по виявленню та класифікації атак на ІТМ. Кожному детектору надається деяка лімітована кількість часу (час життя), впродовж якого він може існувати. Якщо впродовж цього часу детектор не виявляє

аномалій, то він знищується, а на його місце приходить новий детектор. Якщо детектор виявив аномалію, відбувається, так звана, стадія активації. На цій стадії відбувається інформування про виявлену аномалію і її знищення. Детектор, що виявив аномалію, трансформується в детектор імунної пам'яті. Детектори імунної пам'яті характеризуються великим часом життя і рівнем довіри. Такий підхід дозволить змоделювати основні процеси біологічних систем, а також їх взаємодію. Відмінність полягає в способі представлення інформації і структурі НІД.

Отже, в даній роботі запропоновано підхід до організації еволюції детекторів атак на ІТМ в складі системи колективного інтелекту. Використання штучних імунних систем разом з штучними нейронними мережами дозволить підвищити достовірність виявлення і класифікації атак на ІТМ, а також зробити систему захисту гнучкішою і здатною донавчатися та адаптуватися до виявлення нових, раніше невідомих типів атак.

ОСНОВНА ЧАСТИНА

Еволюцію нейромережевих детекторів атак на ІТМ можна представити сукупністю наступних кроків [7]:

1. *Генерація імунних детекторів.* На даному кроці відбувається генерація чотирьох груп НІД відповідно до кількості класів атак з випадковою ініціалізацією вагових коефіцієнтів, де кожна група складається з множини детекторів:

$$D = \left\{ D_i, \quad i = \overline{1, F_d} \right\},\ P = \left\{ P_i, \quad i = \overline{1, F_p} \right\},\ R = \left\{ R_i, \quad i = \overline{1, F_r} \right\},\ U = \left\{ U_i, \quad i = \overline{1, F_u} \right\}, \quad (1)$$

де D_i – i-й НІД для виявлення і класифікації *DoS*-атак;

P_i – i-й НІД для виявлення і класифікації *Probe*-атак;

R_i – i-й НІД для виявлення і класифікації *R2L*-атак;

U_i – i-й НІД для виявлення і класифікації *U2R*-атак;

F – загальна кількість детекторів відповідного типу.

2. *Навчання імунних детекторів.* На даному кроці згенеровані НІД піддаються процесу навчання. Проте механізм навчання такого детектора дещо відрізняється від того, який був представлений в [4, 5]. В даному випадку для виявлення і класифікації атак певного типу може використовуватися не один навчений НІД, а декілька, по-різному навчених детекторів, що дозволяє застосувати процедуру диверсифікації детекторів і відповідно підвищити достовірність виявлення і класифікації атак на ІТМ.

Для навчання НІД одного і того ж типу атаки використовуються різні навчальні вибірки, які генеруються випадковим чином з множини з'єднань, що складаються з певного типу мережевих атак і нормальних з'єднань. В результаті створюється множина різноманітних детекторів.

Нехай N – множина з'єднань, що відносяться до певного типу мережевих атак, а M – множина з'єднань, що відносяться до класу нормальних з'єднань. З них випадковим чином формується множина вхідних образів для навчання i-го детектора:

$$X_i = \begin{bmatrix} X_i^1 \\ X_i^2 \\ \dots \\ X_i^L \end{bmatrix} = \begin{bmatrix} X_{i1}^1 & X_{i2}^1 & \dots & X_{in}^1 \\ X_{i1}^2 & X_{i2}^2 & \dots & X_{in}^2 \\ \dots & & & \\ X_{i1}^L & X_{i2}^L & \dots & X_{in}^L \end{bmatrix}. \quad (2)$$

Відповідно, множина еталонних образів

$$e_i = \begin{bmatrix} e_i^1 \\ \mathrm{e}_i^2 \\ \dots \\ e_i^L \end{bmatrix} = \begin{bmatrix} e_{i1}^1 & e_{i2}^1 \\ e_{i1}^2 & e_{i2}^2 \\ \dots & \\ e_{i1}^L & e_{i2}^L \end{bmatrix}, \quad (3)$$

де L – розмірність навчальної вибірки.

Еталонні вихідні значення для i-го детектора формуються таким чином:

$$e_{i1}^k = \begin{cases} 1, & \textit{якщо } X_i^k \in N \\ 0, & \textit{інакше} \end{cases}$$
$$e_{i2}^k = \begin{cases} 1, & \textit{якщо } X_i^k \in M \\ 0, & \textit{інакше} \end{cases}. \quad (4)$$

Спочатку навчання нейронної мережі проводиться до моменту мінімізації значення сумарної квадратичної помилки:

$$E_i = \frac{1}{2}\sum_{k=1}^{L}\sum_{j=1}^{2}(Y_j^k - e_j^k)^2, \tag{5}$$

де Y_j^k – j-е вихідне значення детектора для k-го вхідного образу;

e_j^k – j-е еталонне значення для k-го еталонного образу.

Потім навчання продовжується до тих пір, поки кількість навчених НІД не стане рівною заданому значенню F.

3. *Відбір імунних детекторів*. Тут для мінімізації виникнення помилкових спрацьовувань, коли нормальне з'єднання приймається за мережеву атаку, всі навчені НІД проходять перевірку на коректність. Для цього, на нейронну мережу подається заздалегідь створена тестова вибірка, що складається тільки з параметрів нормальних з'єднань. Якщо i-й детектор класифікує одне з тестових з'єднань, як атаку, то він знищується, а замість нього генерується і навчається новий детектор. Якщо i-й детектор не генерує помилкові спрацьовування на тестовій вибірці, то він вважається коректним і допускається до аналізу мережевих з'єднань. В результаті утворюється множина НІД для аналізу параметрів мережевих з'єднань, яка, як буде показано далі, може поповнюватися за рахунок детекторів імунної пам'яті та генерування нових детекторів після закінчення часу життя.

4. *Функціонування імунних детекторів*. На цьому кроці вся інформація, що отримується комп'ютером, спочатку аналізується сукупністю НІД (рис. 1), і, якщо жоден з детекторів не виявив аномалію, інформація обробляється операційною системою і відповідним програмним забезпеченням. Крім того, кожен детектор наділяється часом життя, впродовж якого він аналізує мережеві з'єднання. Якщо після закінчення виділеного часу детектор не виявив аномалію, він знищується, а на його місці створюється новий детектор. Механізм наділення детекторів часом життя дозволяє позбуватися від детекторів, які хоч і пройшли успішно стадії навчання і відбору, проте із-за своєї структурної особливості (набору вагових коефіцієнтів) є малопридатними.

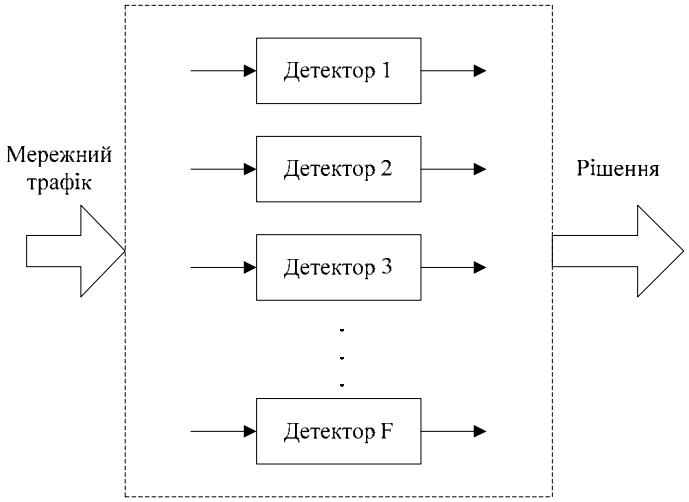

Рис. 1. Сукупність детекторів для аналізу мережного трафіку з метою виявлення і класифікації атак

Якщо мережеве з'єднання класифікується сукупністю НІД як мережева атак то відбувається реагування на атаку (наприклад, блокування з'єднання, в результаті чого воно не допускається до обробки операційною системою і програмним забезпеченням). При цьому видається повідомлення користувачу про спробу атаки на комп'ютерну систему.

5. *Формування імунної пам'яті.* При виявленні і блокуванні мережевої атаки доцільно зберегти її параметри з метою подальшого детального аналізу. Справа в тому, що НІД навчаються на обмеженому наборі даних, які не можуть включати всі ймовірні мережеві атаки. Тому на цьому кроці для підвищення достовірності виявлення і класифікації атак та забезпечення гнучкості системи, параметри мережевого з'єднання, класифікованого як невідома атака, зберігаються і заносяться в навчальну вибірку, тим самим, поповнюючи її актуальними даними. Новостворені детектори вже навчатимуться, зокрема, і на нових даних. Крім цього, на основі детектора, який виявив атаку, створюється новий детектор (операція клонування), який навчається на даних, виділених з виявленої атаки (операція мутації), і вводиться в систему виявлення та класифікації атак на ІТМ. Це дозволяє точніше виділити дану атаку при повторній подібній атаці на комп'ютерну систему. Сукупність детекторів імунної пам'яті зберігає в собі

інформацію про всі невідомі мережеві атаки, направлені в минулому на комп'ютерну систему, і забезпечує високий рівень реагування на повторні спроби атак.

Проведемо експериментальні дослідження еволюції детекторів атак на ІТМ на основі методів штучних імунних систем і нейронних мереж. В якості вхідних даних для НІД використовувалися дані, взяті з бази даних KDD Cup1999 Data [8]. Розмір навчальної вибірки становив 80 векторів (64 – атаки різних типів і 16 – нормальні з'єднання), структура нейронної мережі LVQ – 12-10-2. Оцінка достовірності запропонованого підходу проведена на основі ROC-аналізу [9].

Розглянемо механізм відбору детекторів, що пройшли стадію навчання, який дозволяє позбутися від виникнення помилок другого роду, тобто тих помилок, коли нормальне з'єднання класифікується як мережева атака.

У таблицях 1 і 2 представлено 20 НІД, які пройшли стадію навчання і знаходяться на стадії відбору. У таблиці 1 представлені детектори, які навчалися на атаках класу *dos_neptune*, а в таблиці 2 – детектори, які навчалися на атаках класу *probe_portsweep*.

Таблиця 1

Відбір нейромережевих імунних дедекторів D_i

№	TPR (Se),%	TNR (Sp),%	FNR,%	FPR,%	Accu,%
Детектор D1	100	94,5	0	5,5	97,3
Детектор D2	100	95,6	0	4,4	97,8
Детектор D3	100	95,0	0	5,0	97,5
Детектор D4	100	95,8	0	4,2	97,9
Детектор D5	100	94,7	0	5,3	97,4
Детектор D6	100	99,0	0	1,0	99,5
Детектор D7	100	95,1	0	4,9	97,6
Детектор D8	100	98,7	0	1,3	99,4
Детектор D9	100	98,3	0	1,7	99,2
Детектор D10	100	94,4	0	5,6	97,2

Таблиця 2

Відбір нейромережевих імунних дедекторів P_i

№	TPR (Se),%	TNR (Sp),%	FNR,%	FPR,%	Accu,%
Детектор P1	100	92,2	0	7,8	96,1
Детектор P2	99,6	93,9	0,4	6,1	96,8
Детектор P3	99,8	92,8	0,2	7,2	96,3
Детектор P4	99,3	98,1	0,7	1,9	98,7
Детектор P5	99,9	95,8	0,1	4,2	97,9
Детектор P6	99,4	94,0	0,6	6,0	96,7
Детектор P7	99,9	93,0	0,1	7,0	96,5
Детектор P8	99,0	94,8	1,0	5,2	96,9
Детектор P9	99,1	94,9	0,9	5,1	97,0
Детектор P10	98,7	95,5	1,3	4,5	97,1

Проаналізуємо отримані результати. Як видно з таблиць, деякі детектори (*D1-D10, P1, P5,P7*) достатньо точно виявляють мережеві атаки, на яких відбувалося їх навчання. Проте, при розгляді показника FPR, який відображає рівень помилок другого роду, видно, що він для всіх представлених детекторів в таблицях 1, 2 дуже великий, і такі детектори генеруватимуть помилкові спрацьовування досить часто, що є недопустимим для системи виявлення вторгнень. Такі детектори повинні знищуватися на стадії відбору, результатом функціонування якої повинні бути детектори з низьким рівнем помилок другого роду.

Слід відмітити узагальнюючу властивість НІД. Так, навчений на даних певного класу атак детектор здатний виявляти також атаки, що належать іншому класу. Це відбувається через те, що нормальне мережеве з'єднання за своїми параметрами часто відрізняється від мережевої атаки і вибрана нейронна мережа дозволяє відстежувати ці відмінності.

Результати проведених експериментів по дослідженню узагальнюючої властивості НІД, що дозволяє одному детектору виявляти різні типи атак, представлені в таблицях 3–4.

Таблиця 3

Результати виявлення мережевих атак детекторами 1–3

	Детектор 1 (навчений	Детектор 2 (навчений на	Детектор 3 (навчений

	на *DoS_Back*)	*DoS_Neptune*)	на *DoS_Teardrop*)
Тип атаки	Достовірність виявлення		
DoS-атаки			
Back	100,0	0,0	0,0
Land	0,0	100	81,0
Neptune	99,1	100	100
Pod	0,0	0,0	31,1
Teardrop	0,0	2,7	100
Probe-атаки			
Ipsweep	0,1	6,6	7,0
Nmap	80,5	0,0	96,1
Portsweep	2,1	98,9	97,8
Satan	13,3	88,8	93,9
R2L-атаки			
Guess_passwd	0,0	94,4	0,0
Imap	0,0	83,4	16,7
Spy	100,0	0,0	50,0
Warezclient	1,1	0,3	0,0
U2R-атаки			
Loadmodule	88,9	0,0	11,2
Perl	33,4	0,0	0,0
Rootkit	0,0	0,0	30,0

Таблиця 4

Результати виявлення мережевих атак детекторами 4–6

	Детектор 4 (навчений на *Probe_Nmap*)	Детектор 5 (навчений на *Probe_Portsweep*)	Детектор 6 (навчений на *R2L_Ftpwrite*)
Тип атаки	Достовірність виявлення		
DoS-атаки			
Back	99,1	0,0	0,3
Land	9,5	100	23,8
Neptune	99,9	100	0,0
Pod	12,9	0,0	1,9
Teardrop	11,0	8,8	0,0
Probe-атаки			
Ipsweep	5,7	7,0	1,0
Nmap	100	0,0	0,0
Portsweep	30,8	100	0,1
Satan	96,1	92,2	2,1
R2L-атаки			
Ftp_write	0,0	0,0	100
Guess_passwd	0,0	1,9	5,7
Imap	0,0	75,0	0,0
Multihop	0,0	0,0	57,2
Spy	100	0,0	0,0
Warezclient	0,6	0,2	65,0
Warezmaster	0,0	0,0	90,0
U2R-атаки			
Buffer_overflow	0,0	3,4	83,4
Loadmodule	100	0,0	0,0
Rootkit	0,0	0,0	20,0

Кожен з представлених детекторів навчався на одному певному типі атак (так, детектор 2 навчався на атаці типу *DoS_Neptune*). Після навчання детектори класифікували всі вхідні образи з тестової вибірки. Як видно з представлених таблиць, крім того, що навчені детектори з ймовірністю 100% виявляють той тип атак, на яких відбувалося навчання, вони ще і виявляють атаки з абсолютно інших класів. Причому, деякі типи атак вони виявляють з високою ймовірністю. Звідси випливає, що після навчання і відбору НІД характеризуються властивістю виявляти не тільки відомі, але і невідомі мережеві атаки.

Таким чином, відбувається перехресна перевірка вхідного трафіку всіма детекторами, кожен з яких робить внесок до прийняття рішення про небезпеку або безпеку даного з'єднання, що підвищує надійність системи. Окрім цього, як показали результати експериментів, НІД здатні виявляти не тільки вже відомі атаки, але і невідомі, що є важливою вимогою до сучасних систем безпеки.

Як показано вище, один детектор виявляє різні типи атак, причому навіть ті, які не входили до складу навчальної вибірки. Для оцінки виявляючої властивості детекторів проведемо аналіз залежності виявлення кількості мережевих атак від кількості активних НІД.

У таблиці 5 представлені результати виявлення мережевих атак десятьма різними детекторами.

Таблиця 5

Кількість виявлених атак

Кількість детекторів	Кількість виявлених атак	Кількість детекторів	Кількість виявлених атак
1	108810	6	164087
2	109060	7	164131
3	112214	8	164143
4	162898	9	164143
5	163235	10	164849

Таблиця організована таким чином, що відображає кількість виявлених атак залежно від кількості детекторів. Так, наприклад, детектор під номером 1 виявляє *108810* мережевих атак, два детектори разом вже виявляють *109060* різних атак, три детектори – *112214* і т. д.

Проведемо експериментальні дослідження механізму адаптації НІД.

У таблиці 6 представлені результати адаптації НІД до нових атак в результаті операцій клонування і мутації. В якості батьківського взято детектор, який навчався на атаці типу *dos_land*. Даний детектор 2 виявив невідомі для нього атаки – *r2l_imap* і *probe_portsweep*. Припустимо, що таких атак немає в базі даних, і згенеруємо два нових детектори *A1* і *A2*. Додамо параметри виявлених атак в навчальні вибірки для цих детекторів і навчимо відповідні детектори-клони.

Таблиця 6

Адаптація нейромережевих імунних детекторів *Ai*

	Детектор 2, Sp(TNR)= 99,0%	Детектор A1, Sp(TNR)= 99,1%	Детектор A2, Sp(TNR)= 98,9%
Тип атаки	*Se (TPR),%*	*Se (TPR),%*	*Se (TPR),%*
DoS-атаки			
Land	100,0	100,0	100,0
Neptune	80,9	80,1	80,9
Pod	2,3	0,0	31,8
Teardrop	0,0	2,7	0,0
Probe-атаки			
Ipsweep	7,22	0,2	33,9
Portsweep	15,9	2,6	55,3
Satan	11,0	31,3	11,0
R2L-атаки			
guess_passwd	3,8	1,9	5,7
Imap	83,3	91,7	83,3
Multihop	0,0	0,0	14,3
Warezclient	0,2	1,8	0,2
Warezmaster	0,0	10,0	0,0
U2R-атаки			
Perl	0,0	66,7	0,0
Rootkit	0,0	20,0	0,0

Аналізуючи результати, представлені в таблиці 6, приходимо до висновку, що НІД здатні до адаптації і покращення властивостей виявлення мережевих атак. Так, детектор A1 в 2,8 раза почав краще виявляти атаки класу *probe_satan*, на 8,4% краще атаку типу *r2l_imap*, а також почав виявляти атаки класів *r2l_warezmaster, u2r_perl* і *r2l_rootkit*. А детектор A2 показав кращі результати на атаках класів *dos_pod, probe_ipsweep, probe_portsweep, r2l_multihop*.

Таким чином, експериментально підтверджено, що НІД здатні еволюціонувати з метою адаптації до нових атак на ІТМ. Інтеграція нейромережевих детекторів в ШІС дозволила добитися підвищення

достовірності виявлення і класифікації атак, а також дала можливість зробити систему більш гнучкою і здатною до самонавчання. Це дозволяє системі розвиватися і виявляти нові мережеві атаки на інформаційні ресурси.

ВИСНОВКИ

Запропоновано використати засоби колективного інтелекту для виявлення та класифікації атак на ІТМ. Еволюція детекторів відбувалася на основі базових принципів і механізмів біологічної імунної системи: генерація і навчання імунних детекторів, відбір детекторів, функціонування детекторів, активація і адаптація детекторів до невідомих атак, формування імунної пам'яті.

Розроблено підхід, який базується на інтеграції нейромережевих детекторів в ШІС, що дає можливість НІД еволюціонувати з метою ефективного виявлення та класифікації атак на комп'ютерні системи. Розроблено методику функціонування НІД, яка дозволяє з високою точністю виявляти мережеві атаки, а також зберігати інформацію в детекторах імунної пам'яті про минулі атаки на комп'ютерну систему. Також дозволяє виявляти нові мережеві атаки, вивчати їх та виділяти сигнатури з метою навчання нових детекторів для виявлення і класифікації атак.

Проведено експериментальні дослідження, які підтверджують ефективність запропонованого підходу, оскільки НІД можуть адаптуватися до нових атак на ІТМ за рахунок здійснення операцій клонування і мутації з метою підвищення достовірності їх виявлення і класифікації.

ЛІТЕРАТУРА

1. Bonabeau Eric. Swarm Intelligence: From Natural to Artificial Systems / Eric Bonabeau, Marco Dorigo, Guy Therauaz. – NY: Oxford University Press Inc. – 1999. – 306 p.
2. Haykin S. Neural Networks and Learning Machines / S. Haykin. – Prentice Hall. – 2009. – 906 c.
3. Kohonen T. The self organizing map / T. Kohonen // Proceedings oft he Institute of Electrical and E1ectronics Engineers. – 1990. – Vol. 78. – P. 1464 – 1480.
4. Intelligent system for detection of networking intrusion / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2011). – Prague (Czech Republic), 2011. – Vol.1. – P. 374-377.
5. Sachenko A. Intrusion detection system based on neural networks / A. Sachenko, M. Komar / Scientific Papers of Silesian University of Technology. Organization and Management Series. – Gliwice (Poland), 2014. – Vol. 68. – P. 377-386.
6. Hofmeyr S. Immunity by design: An artificial immune system / S. Hofmeyr, S. Forrest // Gecco. – 1999. – Vol. 2. – P. 1289-1296.
7. Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // Proceedings of the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2013): IEEE international conference, 12–14 September 2013. – Berlin, Germany, 2013. – Vol.2. – P. 665-668.
8. KDD Cup 1999 Data / The UCI KDD Archive, Information and Computer Science. – University of California, Irvine, 1999.
9. Gorban B., Kegl D., Wunsch A., Zinovyev (Eds.), Principal Manifolds for Data Visualisation and Dimension Reduction, LNCSE 58, Springer, Berlin – Heidelberg – New York 2007.