логия определения рациональной структуры информационно-телекоммуникационной системы Государственной пограничной службы Украины на основе использования резервных каналов с учетом показателя эффективности оперативно-служебной деятельности подразделений охраны границы. Данная технология позволяет осуществить рациональный выбор построения сетевой составляющей информационно-телекоммуникационной системы Государственной пограничной службы Украины с резервированием каналов и использованием протокола динамической маршрутизации.

Ключевые слова. Эффективность, информационно-телекоммуникационная система, Государственная пограничная служба Украины, технология повышения эффективности, резервирование каналов.

TECHNOLOGY OF DETERMINING THE RATIONAL STRUCTURE OF THE INFORMATION AND TELECOMMUNICATION SYSTEM OF THE STATE BORDER GUARD SERVICE OF UKRAINE ON THE BASIS OF RESERVE CHANNELS

The effectiveness of the border protection depends on the efficiency of the telecommunications system of the State Border Guard Service of Ukraine. The availability of its individual segments do not meet international requirements for telecommunication systems. Existing methods of increasing of the efficiency of telecommunication systems do not include features of telecommunication system of the State Border Guard Service of Ukraine, namely the impact of its functioning on the effectiveness of the border. The article presents the technology for determining the rational structure of the information and telecommunication system of the State Border Guard Service of Ukraine on the basis of reserve channels taking into consideration the indicator of the operational and service activiti of the border guard units. This technology allows to make the rational choice of building a network component of information and telecommunication system of the State Border Guard Service of Ukraine with the reservation of channels and using the dynamic routing protocol.

Index Terms: Efficiency, information and telecommunication system, the State Border Guard Service of Ukraine, technology efficiency, redundancy channels.

Басараб Олександр Корнійович, ад'юнкт Національної академії Державної прикордонної служби України.
E-mail: a_basarab@ukr.net
Басараб Александр Корнеевич, адьюнкт Национальной академии Государственной пограничной службы Украины.
Basarab Alexander, postgraduate, National Academy of Border Guard Service of Ukraine.

УДК 004.056.53:004.492.3 (045)

ЕВРИСТИЧНІ ПРАВИЛА НА ОСНОВІ ЛОГІКО-ЛІНВИСТИЧНИХ ЗВ'ЯЗОК ДЛЯ ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анна Корченко, Андрій Гізун, Владислава Волянська, Олексій Гавриленко

Недоліком сучасних систем виявлення порушника, побудованих на евристичному принципі виявлення факту порушення інформаційної безпеки є те, що вони в основному орієнтовані на використання таких математичних моделей, які вимагають багато часу на підготовку статистичних даних. Математичні моделі, засновані на експертних підходах в цьому відношенні є більш ефективними, але щоб їх використовувати необхідне формування відповідних правил прийняття рішень. Для вирішення цього завдання в роботі запропонована модель евристичних правил на нечіткій логіці, яка за рахунок використання множин "вплив порушника-параметр", "вплив порушника-набір логіко-лінгвістичних зв'язок" і універсальної моделі еталонів параметрів відображає аномальний стан в інформаційній системі, породжений впливом порушника певної категорії. На основі цієї моделі були розроблені приклади правил для виявлення факту діяльності таких категорій порушника як дезінформатор, хакер, крекер, спамер, бот-зломщик та спам-бот, які можуть практично використовуватися для удосконалення реальних систем виявлення порушника в інформаційних системах.

Ключові слова: *системи виявлення порушника, порушник інформаційної безпеки, ідентифікація, виявлення аномалій в інформаційних системах, нечітка логіка, базова модель ідентифікації порушника, логіко-лінгвістична зв'язка, евристичні правила, експертна оцінка.*

Роль інформаційно-комунікаційних систем в підтримці життєздатності окремих підприємств та національної безпеки держави загалом неупинно зростає, тому актуальність забезпечення безпеки інформаційних систем (ІС) є безумовною. Так одним з найбільш перспективних і пріоритетних

напрямків є захист ІС від впливу зловмисників – порушників інформаційної безпеки. Зокрема в даному напрямку актуальною є проблема розробки систем виявлення порушника (СВП), які дають змогу виявити факт вторгнення в систему та ідентифікувати порушника.

На сьогоднішній день розробляються СВП двох класів: системи, що виявляють факт вторгнення на основі порівняння функціонального стану ІС з набором певних сигнатур (шаблонів) та системи, що ґрунтуються на використані так званих евристичних правил [1]. Головним недоліком першого класу СВП, якого позбавлені системи на базі евристичних правил, є неможливість їх застосування до невідомих атак і як наслідок неможливість практичного використання їх в умовах невизначеності та нечітко формалізованого середовища. Тому, не дивлячись на надзвичайно низький відсоток хибних спрацювань сигнатурних систем, подальший розвиток СВП другого класу на наш погляд є значно перспективнішим.

Існуючі СВП евристичного принципу в основному орієнтовані на використання складних математичних моделей, що вимагають великих часових затрат на формування статистичних даних. Проте, як показано в [2], експертні підходи не мають такої вимоги, що значно спрощує використання даного метода в галузі побудови СВП.

В зв'язку з цим актуальною задачею при розробці СВП є створення моделей виявлення аномального стану ІС, спричиненого діяльністю порушника, на основі використання методів нечіткої логіки та експертних оцінок.

В роботі [3] запропоновані базові параметри для виявлення та ідентифікації порушника в ІС, що дозволяють відображати аномальний стан в ІС, породжений впливом певного типу порушника.

Також в роботі [4] представлена універсальна модель еталонів для групи нечітких параметрів, яка за рахунок даних експертних оцінок і кортежу параметрів дозволяє сформувати множину еталонів лінгвістичних змінних характерних для певного типу порушника. Слід також відмітити подібні роботи [5-7] стосовно виявлення DOS- та DDOS-атак, спуфінгу та скануванню портів.

Застосування даних моделей при побудові СВП евристичного типу пов'язане з необхідністю формування правил направлених на виявлення порушника та його ідентифікацію. Саме тому метою даної роботи є розробка математичної моделі, яка використовується при формуванні відповідних евристичних правил для ідентифікації порушника.

В роботі [3] визначені дві групи параметрів для виявлення та ідентифікації порушника з нечіткою та чіткою природою відповідно. Так нечіткі параметри (Час входу в систему, *Tlog*; Частота запитів на вхід у систему, *Nlog*; Час затрачений на вхід в систему, *TSlog*; Інтенсивність дій, *I*; Процесорний час/завантаженість процесора, *CPU*; Об'єм завантаженої оперативної пам'яті, *Muse*; Кількість виконуваних файлів, *NEF*; Кількість збоїв та помилок, *NEr*; Час виконання процесу/файлу, *RTPr/F*) на першому етапі роботи СВП дають можливість виявити факт наявності порушника в ІС та провести їх попередню ідентифікацію в слабоформалізованому середовищі.

Для підтвердження факту діяльності порушення та остаточного віднесення порушника до певної категорії варто застосовувати чіткі параметри (Ім'я користувача при вході, *UID*; Тип використовуваних файлів при атаці, *AtEF*; Невластиві процеси, *UPr*; Передача файлу в систему, *TrFin*; зміна файлів, *ModF*; копіювання/передача фалів з системи, *TrFout*; Натиснення клавіш клавіатури, *KS*) на другому етапі роботи системи.

Для розв'язання поставленої задачі необхідно побудувати набори евристичних правил, що представляють собою деякі твердження, які засновані на результаті узагальнення певних теоретичних і експериментальних знань (даних) і відображають інтуїтивні судження експертів для забезпечення пошуку раціонального смислового рішення слабоформалізованих задач.

Побудову евристичних правил можна здійснити за допомогою відповідної моделі [7], для створення якої введемо множину лінгвістичних ідентифікаторів

$$\mathrm{LI} = \bigcup_{i=1}^{d} LI = \{LI_1, LI_2, ..., LI_d\}, \qquad (1)$$

де d – кількість елементів множини, необхідних для відображення аномального стану, а LI_i $(i=1, d)$ - елементи LI, кожен з яких приймає одне з текстових значень, що характеризують в лінгвістичній формі рівень аномального стану системи, яке може бути породжене атакуючими діями. Наприклад, при $d=5$ вираз (1) можна визначити як:

$$\mathrm{LI} = \bigcup_{i=1}^{5} LI = \{LI_1, LI_2, LI_3, LI_4, LI_5\} = \{Н, БНВ, БВН, В, К\}, \qquad (2)$$

де LI_1=*Н*, LI_2=*БНВ*, LI_3=*БВН*, LI_4=*В* и LI_5=*К* відповідно відображаються текстовими значеннями "Низький", "Більше низький ніж високий", "Більше високий ніж низький", "Високий" і "Критичний".

Далі на основі множин ідентифікаторів *LI* і набору лінгвістичних або з розширеною назвою логіко-лінгвістичних зв'язок *LC* побудуємо множину евристичних правил

$$\mathrm{ER} = \left\{ \bigcup_{i=1}^{n} ER_i \right\} = \{ER_1,\ ER_2,\ ...,\ ER_n\}, \qquad (3)$$

де ER_i *(i=1,n)* - підмножина можливих правил для виявлення *i*-го аномального стану, породженого *i*-ою атакою, при цьому

$$\begin{aligned} &\bigcup_{i=1}^{n} ER_i = \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{r_n} ER_{ij} \right\} = \{ER_{11}, ER_{12}, ..., ER_{1r_1}\}, \\ &\{ER_{21}, ER_{22}, ..., ER_{2r_2}\}, ..., \{ER_{n1}, ER_{n2}, ..., ER_{nr_n}\}, \end{aligned} \qquad (4)$$

де ER_{ij} *(i=1,n, j=1,rn) - j-е* правило *i*-ої підмножини можливих правил, а r_i *(i=1,n)* – загальна кількість можливих правил, спрямованих на виявлення *i*-ої аномалії.

Зазначимо, що кожному ER_{ij} відповідає евристичний вираз (правило) тобто:

$$\begin{aligned} &\{ER_{11} = (LC_{11} \to LI_{11}), ER_{12} = (LC_{12} \to LI_{12}), ..., \\ &ER_{1r_1} = (LC_{1r_1} \to LI_{1r_1})\}, \{ER_{21} = (LC_{21} \to LI_{21}), \\ &ER_{22} = (LC_{22} \to LI_{22}), ..., ER_{2r_2} = (LC_{2r_2} \to LI_{2r_2})\}, \\ &... \\ &\{ER_{n1} = (LC_{n1} \to LI_{n1}), ER_{n2} = (LC_{n2} \to LI_{n2}), ..., \\ &ER_{nr_n} = (LC_{nr_n} \to LI_{nr_n})\}. \end{aligned} \qquad (5)$$

Узагальнюючи вираз (5) з урахуванням (3) і (4) отримаємо

$$\begin{aligned} &ER = \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{r_i} ER_{ir_j} \right\} = \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{r_i} (LC_{ir_j} \to LI_{ir_j}) \right\} = \\ &\left\{ \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{r_i} ER_{ir_j} = (LC_{ir_j} \to LI_{ir_j}) \right\} \right\}, \end{aligned} \qquad (6)$$

де ER_{ir_j} є r_j-е правило виявлення аномалії породженої *i*-ою атакою, яке буквально інтерпретується як: "Якщо LC_{ir_j} істинно, то рівень аномального стану, який може бути породжений *i*-ою атакою, буде LI_{ir_j} ".

Формування правил зазвичай здійснюється на основі експертного підходу, особливо це важливо в тих випадках, коли необхідно дати перевагу одній з альтернатив, наприклад, при якому LC_{ir_j} (6) результат, пов'язаний з LI_{ir_j} буде найбільш об'єктивно відображати стан системи.

Розглянемо процес формування вибору для набору альтернатив на конкретному прикладі.

Нехай для побудови підмножини правил ER_i використовується r_i логіко-лінгвістичних зв'язок і *d* (1) лінгвістичних ідентифікаторів, один з яких найбільш об'єктивно може відобразити стан середовища щодо наявності аномалії.

Отже, загальна кількість можливих альтернативних рішень - dxr_1, тобто на складання кожного правила ER_{1j} *(j = 1,r1)* необхідно розглянути *d* альтернативних варіантів правил, для вибору одного з яких скористаємося методами визначення коефіцієнтів важливості (КВ) [5].

Скористаємося методом рангових перетворень (РП), оскільки він дозволяє скористатися послугами кількох експертів, в якості вхідних даних застосовуються табличні форми, вихідна функція лінійна, а трудомісткість низька (див. табл. 1 в роботі [5]). Далі, як приклад, визначимо *d=5, r1=3*, тоді

$$\begin{aligned} &\mathrm{LC}_1 = \left\{ \bigcup_{j=1}^{r_1} LC_{1j} \right\} = \{LC_1, LC_2, LC_3\} = \{(\mathrm{t}_{\mathrm{Tlog}} \cong П, \\ &\mathrm{t}_{\mathrm{Nlog}} \cong BC, \mathrm{t}_{\mathrm{TSlog}} \cong B, \mathrm{t}_{\mathrm{CPU}} \cong B, \mathrm{t}_{\mathrm{NEF}} \cong B, \mathrm{t}_{\mathrm{NEr}} \cong B, \\ &\mathrm{t}_{\mathrm{RTPr/F}} \cong ДМ), (\mathrm{t}_{\mathrm{Tlog}} \cong П, \mathrm{t}_{\mathrm{Nlog}} \cong BC, \mathrm{t}_{\mathrm{TSlog}} \cong B, \\ &\mathrm{t}_{\mathrm{CPU}} \cong B, \mathrm{t}_{\mathrm{NEF}} \cong ДВ, \mathrm{t}_{\mathrm{NEr}} \cong B, \mathrm{t}_{\mathrm{RTPr/F}} \cong ДВ), \\ &(\mathrm{t}_{\mathrm{Tlog}} \cong П, \mathrm{t}_{\mathrm{Nlog}} \cong BC, \mathrm{t}_{\mathrm{TSlog}} \cong ДВ, \mathrm{t}_{\mathrm{CPU}} \cong B, \mathrm{t}_{\mathrm{NEF}} \cong ДВ, \\ &\mathrm{t}_{\mathrm{NEr}} \cong B, \mathrm{t}_{\mathrm{RTPr/F}} \cong ДВ)\}, \end{aligned}$$

а в якості значень LI_{1k} *(k = 1,..,5)* скористаємося даними з формули (2).

Таким чином, для кожного LC_{1j} *(j = 1,..,3)* можливі *d=5* фіналів виявлення аномалій, пов'язаних з конкретними значеннями лінгвістичних ідентифікаторів в (2). Найбільш об'єктивний результат визначимо за допомогою методу середніх рангів (СР) [8].

Згідно цього методу, як приклад, скористаємося судженнями 4-х експертів щодо *d=5* можливих результатів ER^k_{1j} *(k = 1,d, j = 1,r1)* по кожному *j*-му правилу.

Наприклад, для першого правила підмножина альтернативних рішень буде

$$\bigcup_{k=1}^{d} ER_{11}^{k} = \left\{ER_{11}^{1}, ER_{11}^{2}, ER_{11}^{3}, ER_{11}^{4}, ER_{11}^{5}\right\} =$$

$$\{(\mathrm{t}_{\mathrm{Tlog}} \cong П, \mathrm{t}_{\mathrm{Nlog}} \cong ВС, \mathrm{t}_{\mathrm{TSlog}} \cong В, \mathrm{t}_{\mathrm{CPU}} \cong В, \mathrm{t}_{\mathrm{NEF}} \cong В,$$
$$\mathrm{t}_{\mathrm{NEr}} \cong В, \mathrm{t}_{\mathrm{RTPr/F}} \cong ДМ) \to Н, (\mathrm{t}_{\mathrm{Tlog}} \cong П, \mathrm{t}_{\mathrm{Nlog}} \cong ВС,$$
$$\mathrm{t}_{\mathrm{TSlog}} \cong В, \mathrm{t}_{\mathrm{CPU}} \cong В, \mathrm{t}_{\mathrm{NEF}} \cong В, \mathrm{t}_{\mathrm{NEr}} \cong В, \mathrm{t}_{\mathrm{RTPr/F}} \cong ДМ)$$
$$\to БНВ, (\mathrm{t}_{\mathrm{Tlog}} \cong П, \mathrm{t}_{\mathrm{Nlog}} \cong ВС, \mathrm{t}_{\mathrm{TSlog}} \cong В, \mathrm{t}_{\mathrm{CPU}} \cong В,$$
$$\mathrm{t}_{\mathrm{NEF}} \cong В, \mathrm{t}_{\mathrm{NEr}} \cong В, \mathrm{t}_{\mathrm{RTPr/F}} \cong ДМ) \to БВН, (\mathrm{t}_{\mathrm{Tlog}} \cong П,$$
$$\mathrm{t}_{\mathrm{Nlog}} \cong ВС, \mathrm{t}_{\mathrm{TSlog}} \cong В, \mathrm{t}_{\mathrm{CPU}} \cong В, \mathrm{t}_{\mathrm{NEF}} \cong В, \mathrm{t}_{\mathrm{NEr}} \cong В,$$
$$\mathrm{t}_{\mathrm{RTPr/F}} \cong ДМ) \to В, (\mathrm{t}_{\mathrm{Tlog}} \cong П, \mathrm{t}_{\mathrm{Nlog}} \cong ВС, \mathrm{t}_{\mathrm{TSlog}} \cong В,$$
$$\mathrm{t}_{\mathrm{CPU}} \cong В, \mathrm{t}_{\mathrm{NEF}} \cong В, \mathrm{t}_{\mathrm{NEr}} \cong В, \mathrm{t}_{\mathrm{RTPr/F}} \cong ДМ) \to К\}.$$

Далі на основі РП визначимо КВ, які відображаються параметром λ. Його мінімальне значення свідчить про більшу перевагу альтернативи, тобто її КВ більш високий.

Для правила ER_{11} зробимо розрахунки значень x_{1j}^{k} і λ_{1j}^{k} по кожному з можливих результатів $ER^{k}{}_{11}$ *(k = 1,5)*: x_{11}^{1} =(1+3+1+2)/4=1,75; x_{11}^{2} =(2+1+3+2)/4=2; x_{11}^{3} =(3+2+2+2)/4=2,25; x_{11}^{4} =(2+4+3+3)/4=3; x_{11}^{5} =*(4+4+* 3+4)/4=3,75.

Значення КВ визначається як $\lambda_{1j}^{k} = x_{1j}^{k} / N$, де N - сума всіх рангів (N=10). За результатами, занесеним в табл. 1 видно, що кращий результат має ER_{11}^{1}, оскільки $\bigwedge_{k=1}^{5} \lambda_{11}^{k} = \lambda_{11}^{k} = 0{,}18$.

Аналогічно зробимо розрахунки для ER_{1j}^{k} *(j=2,3):*

для ER_{12}^{k} – x_{12}^{1} = (2+3+1+2)/4=2**,** x_{12}^{2}= (1+ 2+ 1+ 2)/ 4 = 1,5; x_{12}^{3} = (3+1+2+3) / 4 = 2,25; x_{12}^{4} = (*3*+ 4+ 2+ 2) /4=2,75; x_{12}^{5} =(3+2+3+4)/4=3;

для ER_{13}^{k} – x_{13}^{1} =(2+3+2+4)/4=2,75; x_{13}^{2}= (3+ 2+2 +1)/4 = 2; x_{13}^{3} =(2+3+1+1)/4=1,75; x_{13}^{4}= (3+ 4+3 +4) / 4 = 3,5; x_{13}^{5} =(4+3+2 +4)/4=3,25.

За результатами обчислень (див. табл. 1) видно, що кращий результат для правил ER_{12}, ER_{13}, мають відповідно альтернативні варіанти ER_{12}^{2}, ER_{13}^{3}.

Отримані дані можна використовувати в якості конкретних значень при побудові реальних правил у практичних СВП.

Таблиця 1

Ранги ER_{1j}^{k} і КВ

$ER^{k}{}_{1j}$	j	k	Експерти				$x^{k}{}_{1j}$	$\lambda^{k}{}_{1j}$
			1	2	3	4		
$ER^{1}{}_{11}$	1	1	1	3	1	2	1,75	0,18
$ER^{2}{}_{11}$		2	2	1	3	2	2	0,2
$ER^{3}{}_{11}$		3	3	2	2	2	2,25	0,23
$ER^{4}{}_{11}$		4	2	4	3	3	3	0,3
$ER^{5}{}_{11}$		5	4	4	3	4	3,75	0,38
$ER^{1}{}_{12}$	2	1	2	3	1	2	2	0,2
$ER^{2}{}_{12}$		2	1	2	1	2	1,5	0,15
$ER^{3}{}_{12}$		3	3	1	2	3	2,25	0,23
$ER^{4}{}_{12}$		4	3	4	2	2	2,75	0,28
$ER^{5}{}_{12}$		5	3	2	3	4	3	0,3
$ER^{1}{}_{13}$	3	1	2	3	2	4	2,75	0,28
$ER^{2}{}_{13}$		2	3	2	2	1	2	0,2
$ER^{3}{}_{13}$		3	2	3	1	1	1,75	0,18
$ER^{4}{}_{13}$		4	3	4	3	4	3,5	0,35
$ER^{5}{}_{13}$		5	4	3	2	4	3,25	0,33

Таким чином правило ER_{11} буде мати вигляд:

$$\mathrm{ER}_{11} = (\mathrm{t}_{\mathrm{Tlog}} \cong П, \mathrm{t}_{\mathrm{Nlog}} \cong ВС, \mathrm{t}_{\mathrm{TSlog}} \cong В,$$
$$\mathrm{t}_{\mathrm{CPU}} \cong В, \mathrm{t}_{\mathrm{NEF}} \cong В, \mathrm{t}_{\mathrm{NEr}} \cong В, \mathrm{t}_{\mathrm{RTPr/F}} \cong ДМ) \to Н,$$

що словесно можна інтерпретувати таким чином: "Якщо поточні значення $t_{Tlog}, t_{Nlog}, t_{TSlog}, t_{CPU}, t_{NEF}, t_{NEr}, t_{RTPr/F}$ найбільш близько розташовані до значень $П, ВС, В, В, В, В, ДМ$ відповідно, що входять до $T_{Tlog}, T_{Nlog}, T_{TSlog}, T_{CPU}, T_{NEF}, T_{NEr}, T_{RTPr/F}$, то рівень аномального стану, що породжений атакою порушника (в даному випадку дезінформатором, крекером чи хакером) буде НИЗЬКИЙ".

Сформуємо на основі нечітких параметрів набір евристичних правил ER_1 для виявлення та ідентифікації таких категорій порушника як дезінформатор, крекер, хакер і представимо його в вигляді таблиці 2, позначивши значення параметрів П – підозрілий, Н – нелегітимний, ВС – вище середнього, В – високий (великий), ДВ – дуже великий, ДМ – дуже малий, М – малий.

Використовуючи нечіткі параметри сформуємо набори евристичних правил ER_2 для виявлення та ідентифікації спамера:

$$\mathrm{ER}_2 = \{\mathrm{ER}_{21} = (\mathrm{t}_{\mathrm{I}} \cong С, \mathrm{t}_{\mathrm{CPU}} \cong В, \mathrm{t}_{\mathrm{NEr}} \cong В,$$
$$\mathrm{t}_{\mathrm{RTPr/F}} \cong ДМ) \to БНВ, \mathrm{ER}_{22} = (\mathrm{t}_{\mathrm{I}} \cong С,$$
$$\mathrm{t}_{\mathrm{CPU}} \cong В, \mathrm{t}_{\mathrm{NEr}} \cong В, \mathrm{t}_{\mathrm{RTPr/F}} \cong М) \to Н,$$
$$\mathrm{ER}_{23} = (\mathrm{t}_{\mathrm{I}} \cong В, \mathrm{t}_{\mathrm{CPU}} \cong В, \mathrm{t}_{\mathrm{NEr}} \cong В, \mathrm{t}_{\mathrm{RTPr/F}} \cong$$
$$ДМ) \to В, \mathrm{ER}_{24} = (\mathrm{t}_{\mathrm{I}} \cong В, \mathrm{t}_{\mathrm{CPU}} \cong В,$$
$$\mathrm{t}_{\mathrm{NEr}} \cong В, \mathrm{t}_{\mathrm{RTPr/F}} \cong М) \to БВН\}$$

та ER_3 для виявлення та ідентифікації спам-ботів:

$$ER_3 = \{ER_{31} = (t_I \cong B, t_{CPU} \cong B, t_{NEr} \cong B, t_{RTPr/F} \cong ДМ) \to B, ER_{32} = (t_I \cong B, t_{CPU} \cong B, t_{NEr} \cong B, t_{RTPr/F} \cong M) \to БВН\}.$$

Аналогічно сформуємо набір евристичних правил ER_4 для виявлення та ідентифікації ботазломщика і представимо його в вигляді таблиці 3.

Таблиця 2

Набір правил ER_1

Правило	t_{Tlog}	t_{Nlog}	t_{TSlog}	t_{CPU}	t_{NEF}	t_{Ner}	$t_{RTPr/F}$	Результат
ER_{11}	П	ВС	В	В	В	В	ДМ	Н
ER_{12}	П	ВС	В	В	В	В	М	Н
ER_{13}	П	ВС	В	В	В	В	В	Н
ER_{14}	П	ВС	В	В	В	В	ДВ	Н
ER_{15}	П	ВС	В	В	ДВ	В	ДМ	БНВ
ER_{16}	П	ВС	В	В	ДВ	В	М	Н
ER_{17}	П	ВС	В	В	ДВ	В	В	Н
ER_{18}	П	ВС	В	В	ДВ	В	ДВ	БНВ
ER_{19}	П	ВС	ДВ	В	В	В	ДМ	БНВ
ER_{110}	П	ВС	ДВ	В	В	В	М	БНВ
ER_{111}	П	ВС	ДВ	В	В	В	В	БНВ
ER_{112}	П	ВС	ДВ	В	В	В	ДВ	БНВ
ER_{113}	П	ВС	ДВ	В	ДВ	В	ДМ	БВН
ER_{114}	П	ВС	ДВ	В	ДВ	В	М	БНВ
ER_{115}	П	ВС	ДВ	В	ДВ	В	В	БНВ
ER_{116}	П	ВС	ДВ	В	ДВ	В	ДВ	БВН
ER_{117}	П	В	В	В	В	В	ДМ	БНВ
ER_{118}	П	В	В	В	В	В	М	БНВ
ER_{119}	П	В	В	В	В	В	В	БНВ
ER_{120}	П	В	В	В	В	В	ДВ	БНВ
ER_{121}	П	В	В	В	ДВ	В	ДМ	БВН
ER_{122}	П	В	В	В	ДВ	В	М	БНВ
ER_{123}	П	В	В	В	ДВ	В	В	БНВ
ER_{124}	П	В	В	В	ДВ	В	ДВ	БВН
ER_{125}	П	В	ДВ	В	В	В	ДМ	БВН
ER_{126}	П	В	ДВ	В	В	В	М	БНВ
ER_{127}	П	В	ДВ	В	В	В	В	БНВ
ER_{128}	П	В	ДВ	В	В	В	ДВ	БВН
ER_{129}	П	В	ДВ	В	ДВ	В	ДМ	В
ER_{130}	П	В	ДВ	В	ДВ	В	М	БВН
ER_{131}	П	В	ДВ	В	ДВ	В	В	БВН
ER_{132}	П	В	ДВ	В	ДВ	В	ДВ	В
ER_{133}	Н	ВС	В	В	В	В	ДМ	БНВ
ER_{134}	Н	ВС	В	В	В	В	М	Н
ER_{135}	Н	ВС	В	В	В	В	В	Н
ER_{136}	Н	ВС	В	В	В	В	ДВ	БНВ
ER_{137}	Н	ВС	В	В	ДВ	В	ДМ	БВН
ER_{138}	Н	ВС	В	В	ДВ	В	М	БНВ
ER_{139}	Н	ВС	В	В	ДВ	В	В	БНВ
ER_{140}	Н	ВС	В	В	ДВ	В	ДВ	БВН
ER_{141}	Н	ВС	ДВ	В	В	В	ДМ	БВН
ER_{142}	Н	ВС	ДВ	В	В	В	М	БВН
ER_{143}	Н	ВС	ДВ	В	В	В	В	БВН
ER_{144}	Н	ВС	ДВ	В	В	В	ДВ	БВН
ER_{145}	Н	ВС	ДВ	В	ДВ	В	ДМ	В
ER_{146}	Н	ВС	ДВ	В	ДВ	В	М	БВН
ER_{147}	Н	ВС	ДВ	В	ДВ	В	В	БВН
ER_{148}	Н	ВС	ДВ	В	ДВ	В	ДВ	В
ER_{149}	Н	В	В	В	В	В	ДМ	БВН
ER_{150}	Н	В	В	В	В	В	М	БВН
ER_{151}	Н	В	В	В	В	В	В	БВН
ER_{152}	Н	В	В	В	В	В	ДВ	БВН
ER_{153}	Н	В	В	В	ДВ	В	ДМ	В
ER_{154}	Н	В	В	В	ДВ	В	М	БВН
ER_{155}	Н	В	В	В	ДВ	В	В	БВН
ER_{156}	Н	В	В	В	ДВ	В	ДВ	В
ER_{157}	Н	В	ДВ	В	В	В	ДМ	В
ER_{158}	Н	В	ДВ	В	В	В	М	БВН
ER_{159}	Н	В	ДВ	В	В	В	В	БВН
ER_{160}	Н	В	ДВ	В	В	В	ДВ	В
ER_{161}	Н	В	ДВ	В	ДВ	В	ДМ	К
ER_{162}	Н	В	ДВ	В	ДВ	В	М	В
ER_{163}	Н	В	ДВ	В	ДВ	В	В	В
ER_{164}	Н	В	ДВ	В	ДВ	В	ДВ	К

Таблиця 3

Набір правил ER_4

Правило	t_{Tlog}	t_{Nlog}	t_{TSlog}	t_I	t_{CPU}	t_{NEF}	t_{Ner}	$t_{RTPr/F}$	Результат
ER_{11}	П	ВС	В	В	В	В	В	ДМ	Н
ER_{12}	П	ВС	В	В	В	В	В	М	Н
ER_{13}	П	ВС	В	В	В	В	В	В	Н
ER_{14}	П	ВС	В	В	В	В	В	ДВ	Н
ER_{15}	П	ВС	В	В	В	ДВ	В	ДМ	БНВ
ER_{16}	П	ВС	В	В	В	ДВ	В	М	Н
ER_{17}	П	ВС	В	В	В	ДВ	В	В	Н
ER_{18}	П	ВС	В	В	В	ДВ	В	ДВ	БНВ
ER_{19}	П	ВС	ДВ	В	В	В	В	ДМ	БНВ
ER_{110}	П	ВС	ДВ	В	В	В	В	М	БНВ
ER_{111}	П	ВС	ДВ	В	В	В	В	В	БНВ
ER_{112}	П	ВС	ДВ	В	В	В	В	ДВ	БНВ
ER_{113}	П	ВС	ДВ	В	В	ДВ	В	ДМ	БВН
ER_{114}	П	ВС	ДВ	В	В	ДВ	В	М	БНВ
ER_{115}	П	ВС	ДВ	В	В	ДВ	В	В	БНВ
ER_{116}	П	ВС	ДВ	В	В	ДВ	В	ДВ	БВН
ER_{117}	П	В	В	В	В	В	В	ДМ	БНВ
ER_{118}	П	В	В	В	В	В	В	М	БНВ
ER_{119}	П	В	В	В	В	В	В	В	БНВ
ER_{120}	П	В	В	В	В	В	В	ДВ	БНВ
ER_{121}	П	В	В	В	В	ДВ	В	ДМ	БВН
ER_{122}	П	В	В	В	В	ДВ	В	М	БНВ
ER_{123}	П	В	В	В	В	ДВ	В	В	БНВ
ER_{124}	П	В	В	В	В	ДВ	В	ДВ	БВН
ER_{125}	П	В	ДВ	В	В	В	В	ДМ	БВН
ER_{126}	П	В	ДВ	В	В	В	В	М	БНВ
ER_{127}	П	В	ДВ	В	В	В	В	В	БНВ
ER_{128}	П	В	ДВ	В	В	В	В	ДВ	БВН
ER_{129}	П	В	ДВ	В	В	ДВ	В	ДМ	В
ER_{130}	П	В	ДВ	В	В	ДВ	В	М	БВН
ER_{131}	П	В	ДВ	В	В	ДВ	В	В	БВН
ER_{132}	П	В	ДВ	В	В	ДВ	В	ДВ	В
ER_{133}	Н	ВС	В	В	В	В	В	ДМ	БНВ
ER_{134}	Н	ВС	В	В	В	В	В	М	Н
ER_{135}	Н	ВС	В	В	В	В	В	В	Н
ER_{136}	Н	ВС	В	В	В	В	В	ДВ	БНВ
ER_{137}	Н	ВС	В	В	В	ДВ	В	ДМ	БВН
ER_{138}	Н	ВС	В	В	В	ДВ	В	М	БНВ
ER_{139}	Н	ВС	В	В	В	ДВ	В	В	БНВ
ER_{140}	Н	ВС	В	В	В	ДВ	В	ДВ	БВН
ER_{141}	Н	ВС	ДВ	В	В	В	В	ДМ	БВН
ER_{142}	Н	ВС	ДВ	В	В	В	В	М	БВН
ER_{143}	Н	ВС	ДВ	В	В	В	В	В	БВН
ER_{144}	Н	ВС	ДВ	В	В	В	В	ДВ	БВН
ER_{145}	Н	ВС	ДВ	В	В	ДВ	В	ДМ	В
ER_{146}	Н	ВС	ДВ	В	В	ДВ	В	М	БВН
ER_{147}	Н	ВС	ДВ	В	В	ДВ	В	В	БВН
ER_{148}	Н	ВС	ДВ	В	В	ДВ	В	ДВ	В
ER_{149}	Н	В	В	В	В	В	В	ДМ	БВН
ER_{150}	Н	В	В	В	В	В	В	М	БВН
ER_{151}	Н	В	В	В	В	В	В	В	БВН
ER_{152}	Н	В	В	В	В	В	В	ДВ	БВН
ER_{153}	Н	В	В	В	В	ДВ	В	ДМ	В
ER_{154}	Н	В	В	В	В	ДВ	В	М	БВН
ER_{155}	Н	В	В	В	В	ДВ	В	В	БВН
ER_{156}	Н	В	В	В	В	ДВ	В	ДВ	В
ER_{157}	Н	В	ДВ	В	В	В	В	ДМ	В
ER_{158}	Н	В	ДВ	В	В	В	В	М	БВН
ER_{159}	Н	В	ДВ	В	В	В	В	В	БВН
ER_{160}	Н	В	ДВ	В	В	В	В	ДВ	В
ER_{161}	Н	В	ДВ	В	В	ДВ	В	ДМ	К
ER_{162}	Н	В	ДВ	В	В	ДВ	В	М	В
ER_{163}	Н	В	ДВ	В	В	ДВ	В	В	В
ER_{164}	Н	В	ДВ	В	В	ДВ	В	ДВ	К

На другому етапі після застосування евристичних правил, побудованих на базі нечітких параметрів, слід застосувати правила, розроблені на основі чітких параметрів, для верифікації прийнятого рішення та проведення остаточної категоризації особи порушника. Так вони матимуть вигляд:

$$D = \{\text{UID} = 1, \text{AtEF} = \text{PHP or Java-script}, \text{UPr} = 1, \text{TrFin} = 1, \text{ModF} = 1, \text{TrFout} = 0, \text{KS} = 1\}$$

- для дезінформатора;

$$S = \{\text{UID} = 0, \text{AtEF} = \text{PHP}, \text{UPr} = 1, \text{TrFin} = 1, \text{ModF} = 0, \text{TrFout} = 0, \text{KS} = 1\}$$

- для спамера;

$$C = \{\text{UID} = 1, \text{AtEF} = \text{.exe, .com}, \text{UPr} = 1, \text{TrFin} = 1, \text{ModF} = 1, \text{TrFout} = 1, \text{KS} = 1\}$$

- для крекера;

$$H = \{\text{UID} = 1, \text{AtEF} = \text{script}, \text{UPr} = 1, \text{TrFin} = 0, \text{ModF} = 1, \text{TrFout} = 1, \text{KS} = 1\}$$

- для хакера;

$$SB = \{\text{UID} = 0, \text{AtEF} = \text{PHP}, \text{UPr} = 1, \text{TrFin} = 1, \text{ModF} = 0, \text{TrFout} = 0, \text{KS} = 0\}$$

- для спам-бота;

$$B = \{\text{UID} = 0, \text{AtEF} = \text{script}, \text{UPr} = 1, \text{TrFin} = 0, \text{ModF} = 1, \text{TrFout} = 1, \text{KS} = 0\}$$

- для бота-зломщика.

Висновки. Запропонована в роботі модель евристичних правил з застосуванням нечіткої логіки для першої групи правил та звичайної логіки для другої групи дозволяє за рахунок використання множини "вплив порушника-параметр", "вплив порушника-набір логіко-лінгвістичних зв'язок" і універсальної моделі еталонів параметрів відобразити аномальний стан в ІС, породжений впливом порушника інформаційної безпеки певного типу. На основі цієї моделі були розроблені приклади правил для виявлення і ідентифікації діяльності дезінформатора, спамера, крекера, хакера, спам-бота та бота-зломщика, які можуть бути використані для удосконалення існуючих чи розробки нової СВП.

ЛІТЕРАТУРА

[1]. Корт С.С. Структура систем обнаружения нарушителя (СОН) [Електронній ресурс]: стаття / С. С. Корт. – Режим доступу: http://www.ssl.stu.neva.ru/sam/.

[2]. Корченко А.Г. Построение систем защиты информации на нечетких множествах : Теория и практические решения / А.Г.Корченко. – К. : МК-Пресс, 2006. – 320 с.

[3]. Гізун А.І. Основні параметри для ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, В.О. Риндюк, С.О. Гнатюк // Захист інформації. – 2013. –№1 (58). – С.66-75.

[4]. Волянська В.В. Моделі еталонів лінгвістичних змінних для систем виявлення та ідентифікації порушника інформаційної безпеки // В.В. Волянська, А.І. Гізун, В.О. Гнатюк / Безпека інформації. – №1 (19). – 2013. – С. 13-21.

[5]. Модели эталонов лингвистических переменных для систем выявления атак / М.Г. Луцкий, А.А. Корченко, А.В. Гавриленко, А.А Охрименко // Захист інформації. – 2012. – №2 (55). – С. 71-78.

[6]. Корченко А.О. Система виявлення аномалій на основі нечітких моделей / А.О. Корченко, Є.В. Паціра, В.В. Волянська // Сучасні тренажерно-навчальні комплекси та системи : Зб. наук. праць. – Л.: Інституту проблем моделювання в енергетиці НАН України ім. Г.Є. Пухова, 2007. – Т.2. – С. 56 – 60.

[7]. Корченко А.А. Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах / А.А. Корченко, // Захист інформації. — 2012. — №4 (57). — С. 109-115.

[8]. Горніцька Д.А. Визначення коефіцентів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В Волянська, А.О. Корченко // Захист інформації. – 2012. – №1 (54) . – С. 108-121.

REFERENCES

[1]. Kort S.S. The structure of intruder detection systems [Electronic resource]: abstract, S.S. Kort., Mode of access: http://www.ssl.stu.neva.ru/sam/

[2]. Korchenko A.G. Development of the security systems on fuzzy sets. Theory and practical solutions, A.G. Korchenko, K.: "MK-Press", 2006, 320 P.

[3]. Gizun A.I. Гізун A.I The main parameters to identify the intruder of information security, A.I. Gizun, V.V. Volyanska, V.O. Ryndyuk, S.O. Gnatyuk, Ukrainian Information Security Research Journal., 2013., №1 (58)., P.66-75.

[4]. Volyanska V.V. Models of standards of linguistic variables for detection and identification the intruder of information security, V.V. Volyanska, A.I. Gizun, V.O. Gnatyuk, Ukrainian Scientific Journal of Information Security., №1 (19)., 2013., P. 13-21.

[5]. Models of standards of linguistic variables for the attacks detection systems, M.G. Lutskyi, A.A. Korchenko, A.V. Gavrylenko, A.A Ohrimenko, Ukrainian Information Security Research Journal., 2012., №2 (55)., P. 71-78.

[6]. Korchenko A.O. Anomaly detection system based on fuzzy models, A.O. Korchenko, Ye.V. Patsira, V.V. Volyanska, Modern trainer and educational complexes and systems., L.: Institute for Modelling

in Energy NAS of Ukraine named. G.Ye. Pukhov, 2007., T.2., P. 56 – 60.
[7]. Korchenko A.A. The model of heuristic rules on the logical-linguistic bundles to detect anomalies in computer systems, A.A. Korchenko, Information Security Research Journal., 2012., №4 (57)., P. 109-115.
[8]. Gornits'ka D.A. Coefficients determining of importance for the expert assessment in information security, D.A. Gornits'ka, V.V. Volyanska, A.O. Korchenko, Information Security Research Journal., 2012., №1 (54)., P. 108-121

ЕВРИСТИЧНІ ПРАВИЛА НА ОСНОВІ ЛОГІКО-ЛІНВИСТИЧНИХ ЗВ'ЯЗКІВ ДЛЯ ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Недостатком современных систем обнаружения нарушителя, построенных на эвристическом принципе обнаружения факта нарушения информационной безопасности является то, что они в основном ориентированы на использование таких математических моделей, которые требуют много времени на подготовку статистических данных. Математические модели, основанные на экспертных подходах в этом отношении являются более эффективными, но чтобы их использовать необходимо формирование соответствующих правил по принятию решений. Для решения этой задачи в работе предложена модель эвристических правил на нечеткой логике, которая за счет использования множества "влияние нарушителя-параметр", "влияние нарушителя-набор логико-лингвистических связок" и универсальной модели эталонов параметров отражает аномальное состояние в ИС, порожденное влиянием нарушителя определенной категории. На основе этой модели были разработаны примеры правил для обнаружения факта деятельности таких категорий нарушителя как дезинформатор, хакер, крекер, спамер, бот-взломщик и спам-бот, которые могут практически использоваться для усовершенствования реальных систем обнаружения нарушителя в информационных системах.
Ключевые слова: системы обнаружения нарушителя, нарушитель информационной безопасности, идентификация, выявление аномалий в информационных системах, нечеткая логика, базовая модель идентификации нарушителя, логико-лингвистическая связка, эвристические правила, экспертная оценка.

HEURISTIC RULES BASED ON LOGICAL & LINGUISTIC CONNECTION TO DETECT AND IDENTIFY INFORMATION SECURITY INTRUDERS

Most of existed intruder detection systems based on heuristic principle of information security violation detection and oriented on using mathematical models which need a lot time for statistical data preparation. Mathematical models based on expert approach are more effective but they need adequate rules for decision making. For this problem solving in the paper the model of heuristic rules based on fuzzy logic was proposed. This model uses plurals “intruder influence - parameter”, “intruder influence – set of logical & linguistic connection” and universal model of parameter etalons and allows to display in information system some anomaly generated by influence of some category intruder. On the basis of this model were developed the examples of rules for detection the activity of such categories of intruders as misinformer, hacker, cracker, spammer, bot-braker and spamm-bot. These can be used in practice for the perfection of real intruder detection systems in information systems.
Index Terms: intruder detection systems, information security intruder, identification, anomaly detection in information systems, fuzzy logic, basic intruder identification model, logical and linguistic connection, heuristic rules, expert estimation.

Корченко Анна Олександрівна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: annakor@ukr.net
Корченко Анна Александровна, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Anna Korchenko PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Гізун Андрій Іванович, асистент кафедри безпеки інформаційних технологій Національного авіаційного університету,
E-mail: andriy.gizun@gmail.com
Гизун Андрей Иванович, асистент кафедры безопасности информационных технологий Национального авиационного университета
Gizun Andriy, Assistant of Academic Department of IT-security, National Aviation University

Волянська Владислава Вікторівна, IT-менеджер Apogeum Sp. z o.o. Poland.
E-mail: volyanska.vladyslava@gmail.com
Волянская Владислава Викторовна, ИТ-менеджер ApogeumSp. zo.o. Poland.
Volyanska Vladyslava, IT-manager Apogeum Sp. z o.o. Poland

Гавриленко Олексій Вадимович, к.т.н., доцент кафедри безпеки інформаційних технологій Національного авіаційного університету
E-mail: andriy.gizun@gmail.com
Гавриленко Алексей Вадимович, к.т.н., доцент кафедры безопасности информационных технологий Национального авиационного университета
Gavrylenko Oleksiy, PhD. in Eng., Associate Professor of the Academic Department of IT-security, National Aviation University.