TELECOMMUNICATION SYSTEMS AND NETWORKS

УДК 004 (056.53+73)

ІГОР СУБАЧ,
ВІТАЛІЙ ФЕСЬОХА

МОДЕЛЬ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК НА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ НА ОСНОВІ ОПИСАННЯ АНОМАЛІЙ ЇХ РОБОТИ ЗВАЖЕНИМИ НЕЧІТКИМИ ПРАВИЛАМИ

У статті розглядається актуальна задача захисту інформаційно-телекомунікаційних систем та мереж від кібернетичних атак в умовах їхнього постійного розвитку та поліморфізму шкідливого програмного забезпечення. Проведено аналіз та зроблено висновок про доцільність застосування моделей ідентифікації аномалій, що одночасно оперують якісними і кількісними даними та ґрунтуються на математичному апараті теорії нечітких множин та нечіткого логічного виводу. Зокрема, представлено удосконалену модель виявлення аномалій в роботі інформаційно-телекомунікаційних систем та мереж, яка є подальшим розвитком запропонованої раніше моделі виявлення аномалій на основі нечітких множин та нечіткого логічного виводу. Суть удосконалення полягає у введенні вагових коефіцієнтів для нечітких правил, які описують аномалії, що можуть виникнути під час функціонування інформаційно-телекомунікаційних систем та мереж в результаті несанкціонованого кібернетичного втручання та після введення яких, задача нечіткої ідентифікації аномалій в роботі інформаційно-телекомунікаційної системи зводиться до знаходження рішення аналітичного виразу, який зв'язує множину параметрів стану системи на основі яких визначається її аномальна поведінка та експертне рішення, яке відповідає їм з урахуванням введених вагових коефіцієнтів для правил. Дане удосконалення забезпечує відображення важливості правил у системі нечіткого логічного виводу, яке ґрунтується на впевненості експерта в кожному обраному прийнятому рішенні щодо ідентифікації аномалій. Доцільність використання запропонованої моделі ґрунтується на результатах її дослідження щодо адекватності процесу виявлення аномалій в роботі інформаційно-телекомунікаційних систем і мереж та точності результатів, які вона забезпечує.

Ключові слова: виявлення аномалій, інформаційно-телекомунікаційні системи та мережі, вагові коефіцієнти, зважені нечіткі лінгвістичні правила, база знань, нечіткий логічний вивід, система виявлення вторгнень.

Постановка проблеми в загальному вигляді. Задача захисту інформаційно-телекомунікаційних систем та мереж (ІТСМ) від зловмисного кібернетичного втручання в їх функціонування в умовах постійного розвитку та поліморфізації шкідливого (шпигунського) програмного забезпечення вимагає застосування механізмів ідентифікації кібернетичних вторгнень (КВ), спроможних виявляти нові підходи, форми, способи та/або методи їх компрометації.

Одним з найефективніших підходів до вирішення даної задачі є концепція застосування систем виявлення (запобігання) вторгнень (СВВ/СЗВ) в аспекті детектування аномальної поведінки в ІТСМ на основі певних критеріальних ознак (наприклад, телеметрії мережевого трафіку, *log (pcap)*-файлів СВВ або їх комбінації) [1].

Для ідентифікації аномалій в ІТСМ в руслі викладеного є доцільним застосування моделей, які одночасно оперують якісними і кількісними даними для отримання обґрунтованих рішень та при відносно низькій обчислювальній складності і високій стійкості, відповідають вимогам верифікації та адаптації: гібридизація підходів математичного апарату теорії нечітких множин, нечіткого логічного виводу і експертних систем [2].

Досвід дослідної експлуатації моделей, що реалізовані на основі застосування даного підходу демонструє ефективність щодо точності виявлення КВ (співвідношення виявлених вторгнень до усіх на тестовому наборі) близької 0.9 [3].

Проте, адекватність та точність такої моделі залежить від кваліфікації експертів з кібернетичної безпеки, оскільки саме вони визначають тип та якість налаштування функцій належності усіх (вхідних/вихідних) досліджуваних лінгвістичних змінних предметної області для ідентифікації аномалій.

Це обумовлює актуальність подальших досліджень, які полягають у підвищенні адекватності моделі виявлення аномалій в ІТСМ та точності її результатів.

Аналіз останніх досліджень і публікацій [1] - [6] показує що на етапі формулювання експертом лінгвістичних правил, які утворюють нечітку базу знань (БЗ) про аномалії, що можуть виникнути під час функціонування ІТСМ, впевненість експерта в тому чи іншому правилі може бути різною. Якщо одне правило, на його думку, може служити в якості безперечної істини, то інше правило у того ж експерта може викликати деяку неоднозначність висновку. Оскільки саме від цього етапу залежить подальша ефективність застосування досліджуваної моделі та точність її результатів виявлення аномалій у ІТСМ, то виникає задача її удосконалення шляхом відображення ступенів важливості (значимості) правил у БЗ з суб'єктивної точки зору експерта.

Метою статті є підвищення ефективності застосування моделі виявлення аномалій в ІТСМ, що побудована на основі нечітких множин та нечіткого логічного виводу, в процесі ідентифікації кібернетичних атак.

Виклад основного матеріалу дослідження. Для досягнення поставленої мети, доцільно застосувати підхід, який представлено у [4]. Суть даного підходу полягає у введенні вагових коефіцієнтів для нечітких лінгвістичних правил опису аномалій у БЗ, що можуть виникнути під час функціонування ІТСМ – чисел з інтервалу [0, 1], які характеризують їх важливість у системі нечіткого логічного виводу, ґрунтуючись на впевненості експерта в кожному обраному для прийняття рішення правилі.

Так, після введення вагових коефіцієнтів задача нечіткої ідентифікації аномалій в ІТСМ зводиться до знаходження рішення аналітичного виразу з урахуванням введених вагових коефіцієнтів (ваг правил) – *w*:

$$X^* = (x_1^*, x_2^*, ..., x_n^*) \to y = (a_1^{jk_j}, a_2^{jk_j}, ..., a_n^{jk_j}) \in D = (d_1, d_2, ..., d_n),\ i = \overline{1,n},\ j = \overline{1,m}, \qquad (1)$$

де $X = (x_1, x_2, ..., x_n)$ – множина параметрів опису стану ІТСМ (телеметрії мережевого трафіка, *log (pcap)*-файлів СВВ, показників стану апаратної складової ІТСМ або їх комбінація), на основі яких буде визначатись стан ІТСМ на предмет встановлення факту аномальної поведінки;

y – лінгвістичний опис експертного рішення $d_j \in D$ (висновку) для деякого фіксованого вектора значень вищевказаної множини параметрів $X^* = (x_1^*, x_2^*, ..., x_n^*)$;

jk_j – номери комбінацій значень x_i параметрів опису стану ІТСМ, які відповідають значенню d_j.

Відповідно, знання фахівця з кібернетичної безпеки у модифікованій нечіткій базі правил може бути представлено у вигляді композиційної табл. 1, у якій використано такі позначення:

x_n – вхідна лінгвістична змінна, що відповідає певному досліджуваному параметру опису стану ІТСМ (телеметрії мережевого трафіка, *log (pcap)*-файлів СВВ, показників стану апаратної складової ІТСМ або їх комбінація);

$a_i^{mk_m}$ – нечіткий терм змінної x_n (значення досліджуваного параметра);

d_m – терм нечіткого логічного рішення для лінгвістичної вихідної змінної y на основі множини досліджуваних параметрів.

Таблиця 1 – Композиційна таблиця знань модифікованої нечіткої БЗ

Номер вхідної комбінації	Вхідні змінні (телеметрія мережевого трафіку)				Ваговий коефіцієнт	Вихідна змінна y (висновок)
	x_1	x_2	… x_i …	x_n		
11 12 … $1k_1$	a_1^{11} a_1^{12} … $a_1^{1k_1}$	a_2^{11} a_2^{12} … $a_2^{1k_1}$	… a_i^{11} … … a_i^{12} … … … … … $a_i^{1k_1}$ …	a_n^{11} a_n^{12} … $a_n^{1k_1}$	w_{11} w_{12} … w_{1k_1}	d_1
…	…	…	…	…	…	…
$j1$ $j2$ … jk_j	a_1^{j1} a_1^{j2} … $a_1^{jk_j}$	a_2^{j1} a_2^{j2} … $a_2^{jk_j}$	… a_i^{j1} … … a_i^{j2} … … … … … $a_i^{jk_j}$ …	a_n^{j1} a_n^{j2} … $a_n^{jk_j}$	w_{j1} w_{j2} … w_{jk_j}	d_j
…	…	…	…	…		…
$m1$ $m2$ … mk_m	a_1^{m1} a_1^{m2} … $a_1^{mk_m}$	a_2^{m1} a_2^{m2} … $a_2^{mk_m}$	… a_i^{m1} … … a_i^{m2} … … … … … $a_i^{mk_m}$ …	a_n^{m1} a_n^{m2} … $a_n^{mk_m}$	w_{m1} w_{m2} … w_{mk_m}	d_m

Таким чином, функціональна залежність між досліджуваною обраною множиною параметрів та відповідним прийнятим рішенням про наявність аномалій в ІТСМ з врахуванням введених вагових коефіцієнтів правил формалізується у вигляді наступної системи нечітких логічних тверджень типу „ЯКЩО-ТО, ІНАКШЕ”, побудованої на базі табл. 1:

ЯКЩО ($x_1 = a_1^{11}$) І ($x_2 = a_2^{11}$) І…І ($x_n = a_n^{11}$) (з вагою w_{11}) АБО

($x_1 = a_1^{12}$) І ($x_2 = a_2^{12}$) І…І ($x_n = a_n^{12}$) (з вагою w_{12}) АБО

($x_1 = a_1^{1k_1}$) І ($x_2 = a_2^{1k_1}$) І…І ($x_n = a_n^{1k_1}$)(з вагою w_{1k_1}) ТО

$y = d_1$, ІНАКШЕ

ЯКЩО ($x_1 = a_1^{21}$) І ($x_2 = a_2^{21}$) І…І ($x_n = a_n^{21}$) (з вагою w_{21}) АБО

($x_1 = a_1^{22}$) І ($x_2 = a_2^{22}$) І…І ($x_n = a_n^{22}$) (з вагою w_{22}) АБО

($x_1 = a_1^{2k_2}$) І ($x_2 = a_2^{2k_2}$) І…І ($x_n = a_n^{2k_2}$)(з вагою w_{2k_2}) ТО

$y = d_2$, ІНАКШЕ

ЯКЩО ($x_1 = a_1^{m1}$) І ($x_2 = a_2^{m1}$) І…І ($x_n = a_n^{m1}$) (з вагою w_{m1}) АБО

($x_1 = a_1^{m2}$) І ($x_2 = a_2^{m2}$) І…І ($x_n = a_n^{m2}$) (з вагою w_{m2}) АБО

($x_1 = a_1^{mk_m}$) І ($x_2 = a_2^{mk_m}$) І…І ($x_n = a_n^{mk_m}$)(з вагою w_{mk_m}) ТО

$y = d_m$.

З використанням операцій U (АБО), I (І) вищеописана система логічних висловлювань приводиться до наступного вигляду:

$$\bigcup_{p=1}^{k_j} \left\{ w_{jp} \left[\bigcap_{i=1}^{n} (x_i = a_i^{jp}) \right] \right\} \to y = d_j,\ j = \overline{1,m} \qquad (2)$$

Розрахунок значень багатомірних функцій належності для всіх фахових рішень опису аномалій, що можуть виникнути в ІТСМ при фіксованих значеннях вхідних вказаних вище досліджуваних параметрів представлено у вигляді наступної системи нечітких логічних рівнянь із заміною їх лінгвістичних термів відповідними функціями належності, а операції I та U – на $\wedge$ та $\vee$:

$$\mu^{d_j}\left(x_1, x_2, ..., x_n\right) = \bigvee_{p=1}^{k_j}\left\{ w_{jp}\left[\bigwedge_{i=1}^{n} \mu^{jp}(x_i) \right] \right\},\ j = \overline{1,m} \tag{3}$$

де $\wedge$ – нечітке логічне І, $\vee$ – нечітке логічне АБО.

Оскільки, операціям $\vee$ и $\wedge$ в теорії нечітких множин відповідають операції *max* і *min*, отримуємо:

$$\mu^{d_j}\left(x_1, x_2, ..., x_n\right) = \max_{p=\overline{1,k_j}}\left\{ w_{jp} \min_{i=\overline{1,n}}\left[\bigwedge_{i=1}^{n} \mu^{jp}(x_i) \right] \right\},\ j = \overline{1,m} \tag{4}$$

Таким чином, в якості прийнятого рішення про стан ІТСМ на основі фіксованого вектора вхідних параметрів (телеметрії мережевого трафіка, *log (pcap)*-файлів СВВ, показників стану апаратної складової ІТСМ або їх комбінації) обирається результат з максимальним значенням, отриманим внаслідок згортки функцій приналежності термів нечітких правил опису аномалій та відповідних їм ваговим коефіцієнтам.

Як приклад, розглянемо кібернетичну атаку (КА), відому під назвою "*back*" типу *DoS* на деякий *web*-сервер, метою якої є блокування його сервісу великим потоком некоректних запитів. Намагаючись обробити ці запити, сервер стає неспроможним обслуговувати запити від користувачів системи [7].

Опишемо можливі стани та варіанти відмови даного *web*-серверу в обслуговуванні користувачів (неможливість надання інформаційних послуг):

d_1 – нормальний стан мережевої служби *web*-серверу з впевненістю експерта – 1;

d_2 – відсутність КА, відмова в обслуговуванні внаслідок одночасного звертання до *web*-серверу надто великої кількості користувачів з впевненістю експерта – 0.5.

d_3 – відмова в обслуговуванні внаслідок КА "*back*" з впевненістю експерта – 0.6;

d_4 – відмова в обслуговуванні внаслідок КА "*back*" з впевненістю експерта – 0.8;

d_5 – відмова в обслуговуванні внаслідок КА "*back*" з впевненістю експерта – 0.9;

d_6 – відмова в обслуговуванні внаслідок КА "*back*" з впевненістю експерта – 1.

Для ідентифікації даної КА доцільно досліджувати її характерні ознаки в ІТСМ, які представлені у вигляді наступних вхідних лінгвістичних змінних:

count_packages – кількість надходжень пакетів за секунду;

diff_ip – відсоток різних *ip*-адес, з яких надходять пакети;

bad_format – відсоток запитів з некоректним форматом;

processor_load – відсоток завантаження процесорного блоку серверу.

Нечіткі правила опису станів та варіантів відмови в обслуговування розглянутого *web*-серверу з відповідними ваговими коефіцієнтами представлено у табл. 2.

Дослідження ознак КА "*back*" будемо проводити на основі *Z,S* – подібного (початок/кінець діапазону значень), трикутного та трапецеїдального (проміжні значення діапазону значень) типу функцій належності з наступними значеннями:

count_packages – {"Н – низька [0, 400]", "С – середня [350, 550, 800]", "В – велика [700, 1000]"} на універсумі [0, 1000];

diff_ip – {"Н – низький [0, 25]", "нС – нижче середнього [20, 30, 40]", "С – середній [40, 45, 55, 65]", "вС – вище середнього [60, 70, 80]", "В – високий [80, 100]"} на універсумі [0, 100];

bad_format – {"Н – низький [0, 25]", "нС – нижче середнього [20, 30, 40]", "С – середній [40, 45, 55, 65]", "вС – вище середнього [60, 70, 80]", "В – високий [80, 100]"} на універсумі [0, 100];

processor_load – {“Н – низький [0, 25]”, “нС – нижче середнього [20, 30, 40]”, “С – середній [40, 45, 55, 65]”, “вС – вище середнього [60, 70, 80]”, “В – високий [80, 100]”} на універсумі [0, 100].

Таблиця 2 – Нечіткий опис станів та варіантів відмови *web* – сервера

Вхідні лінгвістичні змінні (ознаки атаки “*back*”)				Ваговий коефіцієнт w	Висновок
count_packages	*diff_ip*	*bad_format*	*processor_load*		y
В	В	Н	Н	1	d_1
В	В	Н	В	0.5	d_2
В	В	нС	В	0.6	d_3
В	В	С	В	0.8	d_4
В	В	вС	В	0.9	d_5
В	В	В	В	1	d_6

Функції належності для деякого фіксованого вектора значень вхідних змінних, що відповідають ознакам здійснення КА “*back*”: X^*=<count_packages*, *diff_ip**, *bad_format**, *processor_load**> = <901, 93, 24, 89> представлено у зведеній табл. 3:

Таблиця 3 – Результати обчислень ступеню належності вхідного вектора

	x_i^*	$\mu^H(x_i^*)$	$\mu^{нC}(x_i^*)$	$\mu^C(x_i^*)$	$\mu^{вC}(x_i^*)$	$\mu^B(x_i^*)$
count_packages	901	0		0		0.67
diff_ip	93	0	0	0	0	0.65
bad_format	24	0.96	0.20	0	0	0
processor_load	89	0	0	0	0	0.45

З метою порівняння результатів раніше відомої [2] та удосконаленої моделей ідентифікації аномалій в ІТСМ проведемо розрахунки на основі описаного вхідного вектора ознак X^* для кожної з них. Так, результати розрахунків моделі до удосконалення становлять:

$$\mu^{d_1}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0.96 \wedge 0) = 0.$$

$$\mu^{d_2}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0.96 \wedge 0.45) = 0.45.$$

$$\mu^{d_3}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0.40 \wedge 0.45) = 0.40.$$

$$\mu^{d_4}\left(X^*\right) = \mu^{d_5}\left(X^*\right) = \mu^{d_6}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0 \wedge 0.45) = 0.$$

Отримані дані показують, що відмова в обслуговуванні *web*-сервера відбулася не внаслідок проведення КА, а одночасного звертання до нього надто великої кількості користувачів, згідно отриманого максимального значення μ^{d_2}.

Результати розрахунків удосконаленої моделі (знаходження рішення аналітичного виразу (1) на основі (4)) становлять:

$$\mu^{d_1}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0.96 \wedge 0) * 1 = 0.$$

$$\mu^{d_2}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0.96 \wedge 0.45) * 0.5 = 0.225.$$

$$\mu^{d_3}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0.40 \wedge 0.45) * 0.6 = 0.24.$$

$$\mu^{d_4}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0 \wedge 0.45) * 0.8 = 0.$$

$$\mu^{d_5}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0 \wedge 0.45) * 0.9 = 0.$$

$$\mu^{d_6}\left(X^*\right) = (0.67 \wedge 0.65 \wedge 0 \wedge 0.45) * 1 = 0.$$

У даному випадку, висновок про відмову в обслуговуванні *web*-сервера буде здійснено на основі отриманого максимального значення μ^{d_3}, що відповідає ознакам проведення КА "*back*".

Наведені розрахунки демонструють, що у першому випадку КА "*back*" не було ідентифіковано (експертне рішення з максимальним значенням функції належності згідно (4) не відповідає проведенню КА), хоча вектор вхідних параметрів X^* відповідає ознакам її проведення (велика кількість надходження пакетів; великий відсоток різних *ip*-адрес, з яких надходять пакети; великий відсоток завантаження процесорного блоку сервера за наявності невеликого відсотка запитів з некоректним форматом), а у випадку застосування удосконаленої моделі завдяки зваженим правилам, система нечіткого логічного виводу моделі встановила факт здійснення КА "*back*" на основі уточненого максимального значення функції належності рішення щодо проведення атаки.

Таким чином, проведене удосконалення моделі виявлення аномалій на основі нечітких множин та нечіткого логічного виводу підвищує не тільки точність її результатів, а й їх достовірність.

Висновки. Застосування запропонованої моделі виявлення КА, що побудована на основі зважених нечітких правил, які описують аномалії в роботі інформаційно-телекомунікаційних систем, дозволяє підвищити ефективність даного процесу.

Перспективними напрямками подальших наукових досліджень є розробка методики ідентифікації кібернетичних атак на інформаційно-телекомунікаційні мережі на основі розроблених моделей виявлення аномалій в їх роботі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] І.Ю. Субач, В.В. Фесьоха, та Н.О. Фесьоха, "Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій", *Information technology and security*, vol. 5, iss. 1, pp. 29-41, 2017.

[2] І.Ю. Субач, та В.В. Фесьоха, "Модель виявлення аномалій в інформаційно-телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу", *Збірник наукових праць ВІТІ*, № 3, с. 158-164, 2017.

[3] R. Shanmugavadivu, and N. Nagarajan, "Network intrusion detection system using fuzzy logic", *Indian Journal of Computer Science and Engineering (IJCSE),* vol. 2, no. 1, pp. 101-111, 2011.

[4] А.П. Ротштейн, Интеллектуальные технологии идентификации. Винница, Україна: Універсум-Вінниця, 1999.

[5] Ю.І. Мітюшкін, Б.І. Мокін, та О.П. Ротштейн, *Soft Computing: ідентифікація закономірностей нечіткими базами знань*. Вінниця, Україна: Універсум-Вінниця, 2002.

[6] О.Я. Сова, Д.А. Міночкін, П.В. Жук, та В.М. Ошурко, "Методика побудови правил нечітких баз знань інтелектуальних систем управління вузлами радіомереж класу MANET", *Сучасний захист інформації*, № 1, с. 74-85, 2015.

[7] "DoS-атаки. Фильтрация на входе сети: Отражение атак DoS, которые используют подмену IP-адреса отправителя (RFC-2827)", [Електронний ресурс]. Доступно: http://www.warning.dp.ua/comp13.htm. Дата звернення: Серп., 01, 2017.

Стаття надійшла до редакції 31 серпня 2017 року.

REFERENCES

[1] I. Subach, V. Fesokha, and N. Fesokha, "An analysis of existing decisions to prevent intrusion in information and telecommunication networks open on the basis of public licenses", *Information technology and security*, vol. 5, no. 1, pp. 29-41, 2017.

[2] I. Subach, and V. Fesokha, “Model of detection of anomalies in information and telecommunication networks of military management bodies on the basis of fuzzy sets and fuzzy logic output”, *Collection of scientific works of VITI*, no. 3, p. 158-164, 2017.
[3] R. Shanmugavadivu, and N. Nagarajan, “Network intrusion detection system using fuzzy logic”, *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 2, no. 1, pp. 101-111, 2011.
[4] O. Rothstein, *Intelligent Identification Technologies*. Vinnytsya, Uraine: Universum-Vinnitsa, 1999.
[5] I. Mityushkin, B. Mokin, and O. Rothstein. Soft Computing: identification of laws with fuzzy knowledge bases. Vinnytsya, Uraine: Universum-Vinnitsa, 2002.
[6] O. Sova, D. Minochkin, P. Zhuk, and V. Oshurko, “Method for constructing rules for fuzzy knowledge bases of intelligent control systems for radio network nodes in the MANET class”, *Modern information protection*, no. 1, pp. 74-85, 2015.
[7] “DoS attacks. Network filtration: Reflects DoS attacks that use the substitution of the sender's IP address (RFC-2827)”, [Online]. Available: http://www.warning.dp.ua/comp13.htm. Accessed on: Aug., 01, 2017.

ІГОРЬ СУБАЧ,
ВИТАЛИЙ ФЕСЁХА

МОДЕЛЬ ОБНАРУЖЕНИЯ КИБЕРНЕТИЧЕСКИХ АТАК НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ НА ОСНОВЕ ОПИСАНИЯ АНОМАЛИЙ В ИХ РАБОТЕ ВЗВЕШЕННЫМИ НЕЧЕТКИМИ ПРАВИЛАМИ

В статье рассматривается актуальная задача защиты информационно-телекоммуникационных систем и сетей от кибернетических атак в условиях их постоянного развития и полиморфизма вредоносного программного обеспечения. Проведен анализ и сделан вывод о целесообразности применения моделей идентификации аномалий, которые одновременно оперируют качественными и количественными данными и основываются на математической теории нечетких множеств и нечеткого логического вывода. Конкретно, представлена усовершенствованная модель выявления аномалий в работе информационно-телекоммуникационных систем и сетей, которая является дальнейшим развитием предложенной ранее модели выявления аномалий, построенной на основе нечетких множеств и нечеткого логического вывода. Сущность усовершенствования состоит в введении весовых коэффициентов для нечетких правил, описывающих аномалии, которые могут возникнуть во время функционирования информационно-телекоммуникационных систем и сетей в результате несанкционированного кибернетического вмешательства в их работу и, после введения которых, задача нечеткой идентификации аномалий в работе информационно-телекоммуникационной системы сводится к нахождению решения аналитического выражения, связывающего множество параметров состояния системы на основании которых определяется ее аномальное поведение та экспертное решение, соответствующее им, с учетом введенных весовых коэффициентов для правил. Данное усовершенствование обеспечивает отображение важности правил в системе нечеткого логического вывода, которое основывается на уверенности эксперта в каждом принятом решении для идентификации аномалий. Целесообразность использования предложенной модели подтверждается результатами ее исследований на предмет адекватности ее процессу выявления аномалий в работе информационно-телекоммуникационных систем и сетей, а также точности результатов, которые она демонстрирует.

Ключевые слова: выявление аномалий, информационно-телекоммуникационные системы и сети, весовые коэффициенты, взвешенные нечеткие лингвистические правила, база знаний, нечеткий логический вывод, система обнаружения вторжений.

IHOR SUBACH,
VITALII FESOKHA

MODEL OF DETECTING CYBERNETIC ATTACKS ON INFORMATION-TELECOMMUNICATION SYSTEMS BASED ON DESCRIPTION OF ANOMALIES IN THEIR WORK BY WEIGHED FUZZY RULES

The article is devoted to the actual task of protecting information-telecommunication systems and networks from cyber attacks in the conditions of their constant development and polymorphizm of malicious software. The analysis is carried out and a conclusion is made about the expediency of using models of anomaly identification that simultaneously operate with qualitative and quantitative data and are based on the mathematical theory of fuzzy sets and fuzzy logical inference. Specifically, an improved model for the detection of anomalies in the work of information and telecommunication systems and networks is presented, which is a further development of the previously proposed anomaly detection model based on fuzzy sets and fuzzy logic inference. The essence of the improvement is the introduction of weight coefficients for fuzzy rules that describe the anomalies that may arise during the operation of information and telecommunication systems and networks as a result of unauthorized cybernetic interference in their work and, after introduction of which, the problem of fuzzy anomaly identification in the work of the information and telecommunication system reduces to finding a solution of an analytic expression connecting a set of parameters of the state of the system on the basis of Its anomalous behavior is determined by the expert decision corresponding to them, taking into account the introduced weight coefficients for the rules. This improvement ensures that the importance of rules is displayed in a fuzzy inference system, which is based on the expert's confidence in each decision taken to identify anomalies. The expediency of using the proposed model is confirmed by the results of her studies on the adequacy of her process of identifying anomalies in the work of information and telecommunication systems and networks, as well as the accuracy of the results that she demonstrates.

Keywords: anomaly detection, information and telecommunication systems and networks, weighting factors, weighted fuzzy linguistic rules, knowledge base, fuzzy logic conclusion, intrusion detection system.

Ігор Юрійович Субач, доктор технічних наук, доцент, завідувач кафедри кібербезпеки та застосування автоматизованих інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: igor_subach@ukr.net.

Віталій Вікторович Фесьоха, ад'юнкт, Військовий інститут телекомунікацій та інформатизації, Київ, Україна.

E-mail: vitaha.fes@gmail.com.

Игорь Юрьевич Субач, доктор технических наук, доцент, заведующий кафедрой кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Виталий Викторович Фесёха, адъюнкт, Военный институт телекоммуникаций и информатизации, Киев, Украина.

Ihor Subach, doctor of technical science, associate professor, head at the cybersecurity and application of information systems academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Vitalii Fesokha, postgraduate student, Military institute of telecommunications and informatization, Kyiv, Ukraine.