

С. Ю. Гавриленко

Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

РОЗРОБКА МЕТОДУ ІДЕНТИФІКАЦІЇ АНОМАЛЬНОГО СТАНУ КОМП'ЮТЕРНОЇ СИСТЕМИ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Предметом статті є дослідження методів ідентифікації аномального стану комп'ютерних системах. **Метою** статті є розробка методу ідентифікації аномального стану комп'ютерної системи на основі методу нечіткої логіки. **Завдання:** дослідити існуючі методи ідентифікації аномального стану комп'ютерних систем; з метою вибору вхідних даних проаналізувати РЕ-структуру шкідливого та безпечного програмного забезпечення та виділити ознаки; оцінити ознаки за допомогою апарату лінійного програмування для подальшого аналізу; розробити метод ідентифікації стану комп'ютерної системи на основі нечіткої логіки, дослідити та обґрунтувати вибір типу функції приналежності, виконати мінімізацію кількості правил, провести тестування. Використовуваними **методами** є: апарат лінійного програмування та апарат нечіткої логіки. Отримано такі **результати**. Розроблено метод ідентифікації стану комп'ютерної системи на основі нечіткої логіки. Для цього вибрано ознаки шкідливого та безпечного програмного забезпечення та оцінено їх за допомогою апарату лінійного програмування, обґрунтовано вибір типу функції приналежності, виконано мінімізацію кількості правил. Проведено тестування запропонованого методу. **Висновки.** Наукова новизна отриманих результатів полягає в наступному: розроблено метод ідентифікації стану комп'ютерної системи на основі нечіткої логіки Мамдані, обґрунтовано вибір типу функції приналежності, виконано мінімізацію кількості правил методом часткового опису за рахунок попарного врахування нечітких множин вхідних змінних, що дозволило збільшити швидкість методу ідентифікації в 5 разів.

Ключові слова: шкідливе програмне забезпечення, РЕ-структура файлу, аномальний стан, комп'ютерна система, нечітка логіка Мамдані.

Вступ

Постановка проблеми. Експерти у області комп'ютерної безпеки відзначають, що обсяги комп'ютерних вірусів та шкідливого програмного забезпечення ростуть із загрозливою швидкістю. На противагу цьому, незважаючи на усі зусилля дослідників і розробників у цій галузі, в даний час не існує такої антивірусної програми, яка могла б ідентифікувати аномальний стан комп'ютерної системи зі стовідсотковою вірогідністю. Саме тому питання розробки та вдосконалення антивірусних засобів залишається актуальною науковою задачею.

Аналіз літератури показав, що існує ряд методів виявлення аномального стану КС. Так методи, що мають за основу байєсовський підхід (Naïve Bayes Approach) [1] є найбільш простими варіантами класифікації даних та не потребують перенавчання. Але вони не враховують комбінований вплив вхідних змінних на результат класифікації та обмежені типом вхідних даних (оброблюються лише дискретні дані). Методи на основі теорії опорних векторів [2] можуть бути використаними тільки для вирішення задач з двома класами ідентифікації. Методи на основі штучних нейронних мереж [3, 4] мають здатність до адаптації та зміні зовнішніх умов шляхом перенавчання, але для них відсутня суворота теорія вибору структури штучної нейронної мережі. Методи на основі генетичних алгоритмів [5, 6] відносно стійкі при попаданні в локальні оптимуми, прості в реалізації, але для них важко знайти точний глобальний оптимум. Вони використовуються для задач оптимізації вже розроблених методів.

Методи на основі регресійного аналізу [7], дозволяють врахувати взаємодію між обраними показниками, але механізм перетворення вихідних даних в кінцевий результат є жорстким, вибір виду конк-

ретної залежності носить суб'єктивний характер (формальна підгонка моделі під емпіричний матеріал), неможливе пояснення причинно-наслідкового зв'язку [8, 9] і, як наслідок, недостатня інформативність результатів, що допускає неоднозначне їх трактування.

Методи на основі кластерного аналізу [10, 11] не завжди інформативні, так як не враховується близькість точок до меж поділу на кластери.

Методи на основі багатofакторного дискримінантного аналізу [12] залежать від особливостей контрольованих показників, їх сенсу, обсягу що призводить до низької точності і швидкості, мають високу ймовірність помилкових спрацьовувань.

Методи виявлення аномального стану системи також погано адаптовані для обробки великих обсягів даних в режимі реального часу [13].

Одним з перспективних напрямків ідентифікації стану КС є використання нечіткої логіки [14–16] для ідентифікації аномалій. Відомий ряд технічних рішень на основі аналізу мережевого трафіку [17–20], а саме формування нечітких еталонів мережевих параметрів і формування евристичних правил для оцінювання мережевої активності [21, 22]. Разом з ним основним недоліком систем нечіткого виведення є їх експоненціальна залежність швидкодії від кількості правил.

Таким чином, проведений аналіз існуючих методів ідентифікації стану комп'ютерних систем показав необхідність адекватного вибору показника аномальної поведінки комп'ютерних систем в умовах зовнішніх впливів і розробки методів оцінки, що відповідає обраним показникам.

Метою статті є розробка методу ідентифікації аномального стану комп'ютерної системи на основі нечіткої логіки та підвищення швидкодії методу за рахунок мінімізації кількості правил.

Результати розробки та досліджень.

Вхідні дані для методу виявлення комп'ютерних вірусів на основі нечіткої логіки сформовані на основі аналізу PE-структури файлу, системних викиликів та ін. Було проаналізовано PE-структуру шкідливого (по 290 файлів типу Worm, Trojan, Backdoor) та безпечного програмного забезпечення та виділено їх ознаки у вигляді API-функцій. Виділені API-функції оцінено за допомогою апарату лінійного програмування з цільовою функцією (1) і обмеженнями (2, 3) та вибрано 25 найбільш значущих API-функцій для подальшого аналізу. Вибрані API-функції об'єднано в групи (A, B, C, D, E) (за ознакою вірогідності приналежності файлів) до вірусних чи нормальних груп (табл. 1):

$$Z = x_1 + x_2 + \dots + x_n \rightarrow \max \quad (1)$$

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \dots + b_{1n}x_n \geq K_a, \\ b_{21}x_1 + b_{22}x_2 + \dots + b_{2n}x_n \geq K_a, \\ \dots \\ b_{m1}x_1 + b_{m2}x_2 + \dots + b_{mn}x_n \geq K_a, \end{cases} \quad (2)$$

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \dots + b_{1n}x_n \leq K_b, \\ b_{21}x_1 + b_{22}x_2 + \dots + b_{2n}x_n \leq K_b, \\ \dots \\ b_{m1}x_1 + b_{m2}x_2 + \dots + b_{mn}x_n \leq K_b, \end{cases} \quad (3)$$

де x_i – коефіцієнт значимості i -ї ознаки, i – бінарне значення, що означає присутність або відсутність i -ї ознаки в j -му зразку, K_a , K_b – початок і кінець діапазону допустимих значень вибірки, які є різними для шкідливого та безпечного ПЗ.

Таблиця 1. Ознаки шкідливого програмного коду у вигляді API-функцій

№	API-функції	% виявлення в шкідливих файлах	% виявлення в безпечних файлах	Різниця	Група
1	callnexthookex	27	75	48	A
2	getcurrentprocessid	39	87	48	
3	getdevicecaps	27	66	39	
4	getmonitorinfo	19	51	32	B
5	getdesktopwindow	25	54	29	
6	shellexecute	37	65	28	C
7	getsysteminfo	26	48	22	
8	unhookwindowshook	28	48	20	
9	setwindowshook	28	47	19	
10	regqueryvalue	76	94	18	
11	wininet	42	22	-20	D
12	gethostbyname	29	3	-26	
13	getstartupinfo	84	55	-29	
14	socket	46	16	-30	
15	registerserviceprocess	31	0	-31	
16	inet addr	35	3	-32	
17	copyfile	81	37	-44	
18	wnet	58	8	-50	E
19	readfile	95	44	-51	
20	writefile	95	44	-51	
21	Pathfindextensionw	62	10	-52	
22	StrStrIW	59	6	-53	
23	Localalloc	97	40	-57	
24	CryptStringtoBinary	64	6	-58	
25	CredEnumerateW	75	15	-60	

У якості методу нечіткого виведення обрано метод Мамдані, який є найбільш прозорим при навчанні. Вхідні лінгвістичні змінні для системи нечіткого виведення за методом Мамдані [23] описано таким кортежем:

$$\langle \alpha, T, X, G, M \rangle,$$

де α – ім'я лінгвістичної змінної (A, B, C, D, E); T – множина значень (термів) вихідної лінгвістичної змінної {«Небезпечна (Danger)», «Невизначена (None)», «Безпечна (Safe)»}; X – множина значень (область міркувань), $X \in [0; 100]$; G – процедура агрегації умов (нових термів); M – функція формування нечіткої множини значень для кожного терма цієї лінгвістичної змінної на універсумі X цієї змінної. Відповідно до отриманих даних, для вибору типу

функції приналежності побудовано дві моделі систем нечіткого виведення: з трапецеїдальною та двосторонньою гаусовою функцією приналежності. Так, область приналежності вхідної змінної «A», для терму «Невизначена (None)» у системі з трапецеїдальною функцією приналежності задано умовою (4), у системі з гаусовою функцією приналежності (рис. 1) – умовою (5).

$$MF(x) = \begin{cases} 1 - \frac{39-x}{12}, & 39 \leq x \leq 51; \\ 1, & 51 < x \leq 57; \\ 1 - \frac{x-57}{9}, & 57 < x \leq 66; \\ 0, & x \notin (39, 66). \end{cases} \quad (4)$$

$$MF(X) = \begin{cases} e^{-(x-51)^2/2a_1^2}, & x < 51, \quad a_1=12; \\ 1, & 51 \leq x \leq 57; \\ e^{-(x-57)^2/2a_2^2}, & x > 57, \quad a_2=9. \end{cases} \quad (5)$$

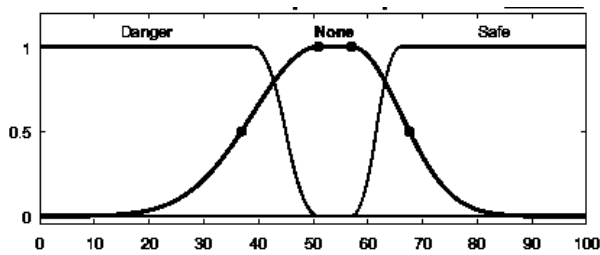


Рис. 1. Графік функцій приналежності (z-подібна, двостороння гаусова, s-подібна) вхідної змінної «А»

В якості вирішальної характеристики для обрання виду функції приналежності було обрано час, який необхідний для виконання обчислень однією та другою функціями. Для цього, системи нечіткого виведення, побудовані за допомогою MatLAB Fuzzy Logic Toolbox, було експортовано в підсистему MatLAB – Simulink (опція Simulink – Profiler Report) та виконано симуляції обома системами нечіткого виведення 20 разів для кожної з систем табл. 2. Отримано, що система нечіткого виведення з використанням трапецеїдальної функції приналежності працює в середньому швидше системи з двосторонньою гаусовою функцією приналежності на 0,06 секунди. Надалі, для моделювання обрано трапецеїдальну функцію приналежності.

База правил формується на основі сформованих умов та висновків, тобто вхідних та вихідних лінгвістичних змінних. Якщо набирати усі правила методом перебору, то база правил даної системи буде містити в собі 243 різні правила. Аналіз бази правил показав що база є надмірною і потребує оптимізації [24]. Для пришвидшення розрахунків, було проведено оптимізацію методом часткового опису. Для цього виконано попарне врахування нечітких множин вхідних змінних системи нечіткого виведення для методу повного перебору. Отримані пари аналізувались незалежно від значень трьох інших входів системи. Правила описувались за таким шаблоном:

– якщо вхідна змінна А = «нечітка множина змінної А» та (логічна операція «&&») вхідна змінна В = «нечітка множина змінної В», тоді вихідна змінна F = «нечітка множина змінної F»:

$$A = \overline{1...3}, B = \overline{1...3}, A \neq B, F = \overline{1...3}.$$

Таким чином було перебрано всі можливі пари нечітких множин вхідних змінних без повторювань, що дозволило значно скоротити кількість правил:

– на першому кроці було порівняно вхід А зі входами В, С, D, E: 9 + 9 + 9 + 9 = 36 правил;

– на другому кроці було порівняно вхід В зі входами С, D, E: 9 + 9 + 9 = 27 правил;

– на третьому кроці було порівняно вхід С зі входами D, E: 9 + 9 = 18 правил;

на четвертому кроці біло порівняно вхід D з входом E: 9 правил. Всього таким підходом отрима-

но: 36 + 27 + 18 + 9 = 90. Фрагмент такої бази правил системи нечіткого виводу наведено на рис. 2.

Таблиця 2. Швидкість ідентифікації з використанням трапецеїдальної та гаусової функції приналежностей

№	Час моделювання, с	
	Трапецеїдальна функція приналежності	Асиметрична гаусова функція приналежності
1	17,56	12,73
2	10,22	10,27
3	9,77	11,59
4	11,98	10,73
5	10,11	11,58
6	10,31	9,97
7	10,14	9,94
8	10,03	10,41
9	10,81	10,86
10	10,17	10,05
11	9,66	10,33
12	9,59	10,67
13	10,22	9,83
14	9,91	10,31
15	9,89	10,22
16	9,58	10,75
17	10,5	10,44
18	10,7	10,98
19	9,97	10,55
20	10,42	10,63
Середнє	10,58	10,64

1. If (A is None) and (B is Danger) then (F is Virus) (1)
2. If (A is None) and (B is None) then (F is None) (1)
3. If (A is None) and (B is Safe) then (F is Safe) (1)
4. If (A is Danger) and (B is Danger) then (F is Virus) (1)
5. If (A is Danger) and (B is None) then (F is Virus) (1)
6. If (A is Danger) and (B is Safe) then (F is None) (1)
7. If (A is Safe) and (B is Danger) then (F is None) (1)
8. If (A is Safe) and (B is None) then (F is Safe) (1)
9. If (A is Safe) and (B is Safe) then (F is Safe) (1)
10. If (A is None) and (C is Danger) then (F is Virus) (1)
11. If (A is None) and (C is None) then (F is None) (1)

Рис. 2. Фрагмент бази правил системи нечіткого виведення

Так як результат акумуляції для кожної вихідної лінгвістичної змінної визначається як об'єднання нечітких множин всіх підвисновків нечіткої бази правил щодо відповідної лінгвістичної змінної, то точність методу після мінімізації кількості правил не зміниться.

Результат оптимізації бази правил, сформованих методом часткового опису (90 правил), показали, що швидкість ідентифікації зростає і складає 1,96 с. проти 10,64 с., табл. 3.

Результати моделювання методу ідентифікації стану КС на основі системи нечіткого виведення Мамдані наведено на рис. 3.

Проведено тестування розробленої системи, яке показало, що ймовірність виявлення шкідливого програмного забезпечення з урахуванням помилкових спрацьовувань, становить 96.5%. рис. 4.

Таблиця 3. Результати моделювання Simulink

№ з/п	Час моделювання, с	№ з/п	Час моделювання, с
1	1,98	3	2
2	2,16	4	1,78
5	1,81	13	2,08
6	1,89	14	2,13
7	1,89	15	1,91
8	1,84	16	1,91
9	1,86	17	1,95
10	1,95	18	2,06
11	2,09	19	1,89
12	1,92	20	2,02
Середнє значення		1,96	

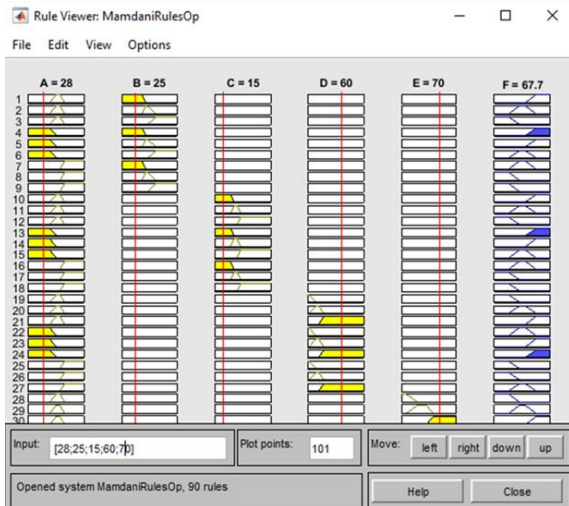


Рис. 3. Моделювання системи нечіткого виведення

Висновки

Розглянуто методи ідентифікації аномального стану комп'ютерних систем. З метою вибору вхідних

даних проаналізовано РЕ-структуру шкідливого та безпечного програмного забезпечення, виділено API-функції для подальшого аналізу та виконано їх оцінку за допомогою апарату лінійного програмування. Розроблено метод ідентифікації стану КС на основі нечіткого виведення Мамдані. Проведено дослідження щодо вибору типу функції приналежності.

Виконано мінімізацію кількості правил методом часткового опису за рахунок попарного врахування нечітких множин вхідних змінних для методу повного перебору, що дозволило збільшити швидкість методу ідентифікації в 5 разів.

Проведено тестування розробленого методу ідентифікації, яке показало, що ймовірність виявлення аномального стану, з урахуванням помилкових спрацьовувань, становить 96.5%.

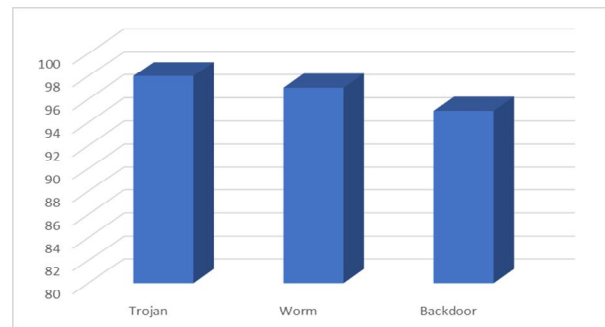


Рис. 4. Результати тестування системи

Подальші дослідження технологій ідентифікації стану об'єктів можуть бути виконані в дослідженні нечіткої кластеризації. Це дозволить одному і тому ж об'єкту належати одночасно кільком кластерам, але з різним ступенем приналежності, що підвищить точність ідентифікації стану комп'ютерної системи.

СПИСОК ЛІТЕРАТУРИ

- Маккаффи Дж. Кластеризация данных с использованием наивного байесовского вывода. [Електронний ресурс], – Режим доступу: <http://msdn.microsoft.com/ru-ru/magazine/jj991980.aspx>.
- Лифшиц Ю. Метод опорных векторов. [Електронний ресурс], – Режим доступу: <http://yury.name/internet/07ianote.pdf>.
- Хайкин С. Нейронные сети: полный курс. М.: Издательский дом "Вильямс", 2006. – 1104 с.
- Семенов С.Г. Защита данных в компьютеризированных управляющих системах (монография). / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко // «LAP LAMBERT ACADEMIC PUBLISHING»: Germany, 2014. – 236 с. Рутковская Д., Пилинский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. М.: Горячая линия – Телеком, 2006. – 452 с.
- Энгельгардт В. В. Генетический алгоритм структурно-параметрической идентификации линейных динамических систем с помехами на входе и выходе / В. В. Энгельгардт // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2013. - № 4 (28). С. 5-18.
- Sen A Regression Analysis. Theory, Methods, and Applications / A. Sen, M. Srivastava, // Springer-Verlag, Berlin, 2011, – 264 p.
- Weedmark David. "The Advantages & Disadvantages of a Multiple Regression Model." Sciencing, 2018, [Електронний ресурс] – Режим доступу: <https://sciencing.com/advantages-disadvantages-multiple-regression-model-12070171.html>.
- Flom Peter. "The Disadvantages of Linear Regression." Sciencing, 2018, [Електронний ресурс], – Режим доступу <https://sciencing.com/disadvantages-linear-regression-8562780.html>. (дата звернення: 04.12.2018)
- Everitt, Brian Cluster analysis. / Everitt, Brian // Chichester, West Sussex, U.K: Wiley, 2011, – 330 p., ISBN 9780470749913, (дата звернення: 04.12.2018).
- Сулов С.А. "Кластерный анализ: сущность, преимущества и недостатки" / С.А. Сулов // Вестник НГИЭИ // Н. Новгород: 2010. – Т. 1, N. 1, С. 51-57.
- Barbara Illowsky Introductory Statistics / Barbara Illowsky, Susan Dean // OpenStax CNX, 2014, – 905 p.
- Касперский К. Играй, как «Лаборатория Касперского»: компания открывает доступ к своей базе знаний о киберугрозах в рамках нового бизнес-сервиса – Режим доступу: https://www.kaspersky.ru/about/press-releases/2017_kompaniya-otkryvaet-dostup-k-svoey-baze-znaniy-o-kiberugrozakh-v-ramkakh-novogo-biznes-servisa.
- Kumar S.V.A. Anomaly based Intrusion Detection using Modified Fuzzy Clustering. International Journal of Interactive Multimedia and Artificial Intelligence. 2017.– № 4(6), pp.54-59. DOI 10.9781/ijimai.2017.469

14. Ghosh S. "Network anomaly detection using a fuzzy rule-based classifier" / S. Ghosh, A. Pal, A. Nag, S. Sadhu and R. Pati, //Computer Communication and Electrical Technology, 2017 , pp. 61 -65.
15. Ali Feizollah. Anomaly Detection Using Cooperative Fuzzy Logic Controller/Conference Paper in Communications in Computer and Information Science · August 2013, pp 220-231, DOI: 10.1007/978-3-642-40409-2_19
16. Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. –К.: 2012. – № 2 (18). С. 80-84.
17. Kuchuk G.A. An Approach To Development Of Complex Metric For Multiservice Network Security Assessment / G.A. Kuchuk, A.A. Kovalenko, A.A. Mozhaev // Statistical Methods Of Signal and Data Processing (SMSDP – 2010): Proc. Int. Conf., October 13-14, 2010.– Kiev: NAU, RED, IEEE Ukraine section joint SP, 2010. – P. 158 – 160.
18. V. Manikandan, V. Porkodi, Amin Salih Mohammed and M. Sivaram (2018), "Privacy preserving data mining using threshold based fuzzy cmeans clustering", *ICTACT Journal On Soft Computing*, 2018, Vol. 09, Issue 01, pp. 1813-1816.
19. Amin Salih Mohammed, D Yuvaraj, M. Sivaram Murugan, V. Porkodi, "Detection and removal of black hole attack in mobile ad hoc networks using GRP protocol", *International Journal of Advanced Computer Research*, vol. 9, no. 6, pp. 1-6, 2018, DOI: <http://doi.org/10.26483/ijarcs.v9i6.6335>
20. Saravana Balaji B., Amin Salih Mohammed, Chiai Al-Atroshi, "Adaptability of SOA in IoT Services – An Empirical Survey", *International Journal of Computer Applications*, vol. 182(31), pp. 25-28, 2018, DOI: <http://doi.org/10.5120/ijca2018918249>
21. Корченко А.А. Система формирования нечетких эталонов сетевых параметров / А.А. Корченко // Захист інформації. – К.: 2013. – Т.15, №3. С. 240-246.
22. Штовба С.Д. Проектирование нечетких систем средствами MATLAB. - М.: Горячая линия-Телеком, 2007. – 288 с.
23. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. - СПб: БХВ-Петербург, 2005. - 736 с.
24. Gavrylenko S. Development of a heuristic antivirus scanner based on the file's PE-structure analysis / S.Yu. Gavrylenko, M.S. Melnyk, V. V. Chelak// Інформаційні технології та комп'ютерна інженерія.– Вінниця: ВНТУ, 2017.– №3 (40), С. 23-29.

Рецензент: д-р техн. наук, проф. К. С. Козелкова,
Державний університет телекомунікацій, Київ
Received (Надійшла) 24.10.2018
Accepted for publication (Прийнята до друку) 09.01.2019

Разработка метода идентификации аномального состояния компьютерной системы на основе нечеткой логики

С. Ю. Гавриленко

Предметом статьи является исследование методов идентификации аномального состояния компьютерных систем. **Целью** статьи является разработка метода идентификации аномального состояния компьютерной системы на основе метода нечеткой логики. **Задачи:** исследовать существующие методы идентификации аномального состояния компьютерных систем; с целью выбора входных данных проанализировать PE-структуру вредного и безопасного программного обеспечения выделить признаки; оценить признаки с помощью аппарата линейного программирования для дальнейшего анализа; разработать метод идентификации состояния компьютерной системы на основе нечеткой логики, исследовать и обосновать выбор типа функции принадлежности, выполнить минимизацию количества правил, провести тестирование. Используемыми **методами** являются: аппарат линейного программирования и аппарат нечеткой логики. Получены следующие **результаты**. Разработан метод идентификации состояния компьютерной системы на основе нечеткой логики. Для этого выбрано признаки вредного и безопасного программного обеспечения и оценены их с помощью аппарата линейного программирования, обоснован выбор типа функции принадлежности, выполнено минимизацию количества правил. Проведено тестирование предложенного метода. **Выводы.** Научная новизна полученных результатов заключается в следующем: разработан метод идентификации состояния компьютерной системы на основе нечеткой логики Мамдани, обоснован выбор типа функции принадлежности, выполнено минимизацию количества правил методом частичного описания за счет парного учета нечетких множеств входных переменных, что позволило увеличить быстроедействие метода идентификации в 5 раз.

Ключевые слова: вредоносное программное обеспечение, PE-структура файла, аномальное состояние, компьютерная система, нечеткая логика Мамдани.

Development of a method for identifying abnormal computer system based on fuzzy logic

S. Gavrilenko

The subject matter of the article is investigation the methods for identifying the anomalous state of computer systems. **The goal** of the article is to develop a method for identifying the anomalous state of a computer system based on the fuzzy logic. **Tasks:** to investigate methods for identifying the anomalous state of computer systems; to analyze the RE-structure of harmful and safe software for selecting input data and select signs; to estimate these signs using a linear programming apparatus; to develop a method for identifying the state of a computer system using fuzzy logic; to investigate and chose the type of the membership function; to minimize the number of rules, to test this method. **The methods** used are: a linear programming apparatus and a fuzzy logic apparatus. The results were as follows. A method for identifying the state of a computer system based on fuzzy logic was developed. The signs of harmful and safe software was selected and evaluated using a linear programming device. The choice of the type of the membership function was well founded and the number of rules was minimized. The proposed method was tested. **Conclusion.** The scientific novelty of the obtaining results is as follows. The investigation for the selection of input data for analysis was conducted. The method of identifying the state of a computer system based on Mamdani fuzzy logic was developed. The choice of the type of membership function was founded, the number of rules using the partial description method by pairwise taking into account fuzzy sets of input variables was minimized. It increase 5 times the speed of the identification method.

Keywords: malware, PE file structure, abnormal state, computer system, Mamdani fuzzy logic.