ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2019. No. 2 (8)

УДК 004.7 DOI: https://doi.org/10.30837/2522-9818.2019.8.036

С. Ю. ГАВРИЛЕНКО

СИНТЕЗ ІДЕНТИФІКАЦІЙНИХ ВИМІРІВ В КОМП'ЮТЕРНІЙ СИСТЕМІ КРИТИЧНОГО ПРИЗНАЧЕННЯ

Предметом дослідження є методи та засоби ідентифікації стану комп'ютерної системи критичного призначення. **Метою** даної статті є проведення аналізу та розробки загальної схеми синтезу ідентифікаційних вимірів в системі ідентифікації стану комп'ютерної системи критичного призначення. У статті вирішені наступні **завдання.** Проаналізовано методи відбору інформативних показників ідентифікації стану та методи синтезу ідентифікаційних вимірів в комп'ютерній системі критичного призначення. У **результаті** проведеного аналізу сформульовано основні оптимізаційні задачі та наведено приклад можливого використання відомого математичного апарату при їх вирішенні. При розв'язанні поставлених завдань були використані **методи** багатокритеріального оцінювання, дискримінантного та кластерного аналізу, математичної статистики та компараторний підхід. Отримані **результати.** Проведені дослідження показали, що загальна схема ідентифікації стану комп'ютерної системи критичного призначення повинна включати методи ідентифікації аномалій та методи ідентифікації зловживань, а завдання ідентифікації аномалій в ній повинно бути вирішено в умовах дуже складних обмежень на достовірність результатів ідентифікації, причому оперативність вирішення цього завдання не повинно бути гірше встановлених керівними документами вимог. В результаті синтезовано загальну схему ідентифікації стану комп'ютерної системи критичного застосування, що відрізняється від відомих комплексним використанням вдосконалених методів ідентифікації, та їх адаптацією до можливих змін вхідних даних; експериментальним шляхом визначено множину можливих вхідних показників для ідентифікації стану; проведено порівняльний аналіз методів ідентифікації стану; отримані графіки часу ідентифікації зловживань у комп'ютерній системі критичного призначення в залежності від кількості реєстрованих даних. **Висновок**: комплексне використання методів ідентифікації аномалій дозволило до 1,9 разів підвищити достовірність ідентифікації, а комплексне використання методів ідентифікації зловживань в комп'ютерних системах критичного застосування дозволило підвищити оперативність ідентифікації до 2 разів.

Ключові слова: ідентифікація стану; комп'ютерна система критичного застосування; ідентифікаційні виміри; ідентифікації зловживань.

Вступ

В ході ідентифікації стану комп'ютерних систем критичного призначення (КСКП) одним із актуальних завдань залишається синтез результатів ідентифікаційних вимірів. При вирішенні та реалізації цього завдання дослідники зустрічаються зі складностями окремих часткових задач, наприклад, визначення найбільш інформативних метрик та їх ранжування, визначення критеріїв ідентифікації, оптимізації за множинами функціональних і вартісних показників тощо. Рішення цих задач передбачає безпосередній розгляд змісту розробленої системи ідентифікації стану КСКП. Для цього необхідно використовувати сукупність моделей, методів та засобів ідентифікації, які описані у [1–3]. Слід відзначити, що методи реалізації функцій ідентифікації стану, що наведені в цих роботах, а також вхідні дані та обмеження, суттєво звужують перелік технологій ідентифікації, що дозволяють ефективно вирішувати поставлені завдання. Отже, предметом дослідження є методи та засоби ідентифікації стану комп'ютерної системи критичного призначення.

Аналіз останніх досліджень і публікацій

Проведений аналіз літератури [1–15] показав, що на даний час існує багато підходів щодо ідентифікації технічних систем. Так, наприклад, в роботах [1, 7] наведено ряд моделей ідентифікації технічних систем, основаних на аналітичному, експериментальному та аналітично-експериментальному методах. Аналітичний метод передбачає отримання математичного опису об'єкта на основі законів фізики, механіки, хімії тощо. Такий підхід дає позитивний результат, якщо даний об'єкт досить простий за структурою і добре вивчений. Якщо ж об'єкт вивчений недостатньо або ж настільки складний, що аналітичний опис його математичною моделлю практично неможливий, то вдаються до експериментальних методів, суть яких зводиться до статистичної обробці технологічних даних. При експериментально-аналітичному методі апріорна модель, отримана аналітичним шляхом, уточняється у відповідних експериментах.

Слід зауважити що у більшості наведених робіт за основу математичної формалізації пропонується обрання систем диференційних рівнянь різного рівня складності. Нажаль, ця загальна класифікація та моделі не дають можливості врахування багатьох факторів, як нештатних ситуацій функціонування КСКП так і зовнішніх впливів. Але вибір структури моделі повинен диктуватися як умовами реалізації, так і вимогою адекватності.

В роботах [8, 9] зроблена спроба усунення вказаних недоліків. В цих роботах вказано, що в умовах апріорної невизначеності інтуїція є однією з складових процесу прийняття рішення про структуру моделі. При цьому на перший план виходить аналіз даних з метою отримання додаткових структурних властивостей даних, що відображають ті чи інші характерні риси системи. В цих роботах пропонується напрям, що дозволяє отримати додаткову інформацію про структуру об'єкта (інформаційний портрет), що задана в просторі "вхід-вихід".

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2019. № 2 (8) ISSN 2524-2296 (online)

Дуже схожий к вищевказаному підхід описаний в роботах [4, 7]. В них математичну інтерпретацію процесу функціонування технічної системи пов'язують з поняттям функціонального стану. У математичній формі ця інтерпретація може бути записана в такому вигляді: $R \subset Q$, де Q – відношення еквівалентності, визначене на множині станів моделі таким чином, щоб множина його класів на цій множині взаємно-однозначно відповідало множині імен цілей в управлінні об'єктом. Всі моделі, що задовольняють даній умові, можуть бути використані для вирішення завдань ситуаційного управління поведінкою об'єктів в просторі їхніх статків. В цих роботах визнається, що функціональний стан – це атрибут детермінованої моделі керованих змін в процесах функціонування технічного об'єкта, котрий:

а) характеризує в моделі стійку і рівноважну фазу цих процесів щодо заданої підмножини впливів зовнішнього середовища і обраного інтервалу часу існування об'єкта;

б) має унікальне ім'я, семантичну інтерпретацію і ідентифікується у значеннях параметрів цих процесів, знання яких і надаються на об'єкт, яким управляють.

Нажаль, вказаний перелік наукових досліджень також має певні обмеження використання, що суттєво ускладнює їх застосування в КСКП. Наприклад, при побудові інформаційних портретів немає чітких правил обрання інформаційних показників, їх градації та рекомендацій при використанні різними методами ідентифікації станів. При формуванні функціональних станів та відповідному математичному опису цього підходу не враховуються залежності змін функціональних станів від відповідних правил прийняття рішень та ін.

Аналіз літератури та проведені дослідження показали, що одним з найбільш ефективних підходів синтезу методів ідентифікації стану КСКЗ може бути компараторний підхід. Дана технологія ретельно досліджена та описана в роботах [1, 7]. Так в роботі [7] визначено, що однією з першочергових задач вважається задача синтезу моделей для скалярного багатокритеріального оцінювання варіантів. При цьому пропонується автоматичне оцінювання та вибір рішень за множиною часткових критеріїв з використанням методології компараторної ідентифікації переваг експертами. Але при вирішенні основного завдання найважливішою задачею стає визначення метрики для їх ранжування. Методологічною основою для побудови метрики пропонується використання теорії корисності [9], відповідно до якої для кожного з рішень з допустимої множини X може бути визначено значення його загальної корисності (цінності) $P(q,x)$, де $q-$ вектор параметрів функції.

Визначення метрики $P(q,x)$ для ранжування рішень з множини $x \in X$ допустимих рішень полягає в розв'язанні задачі ідентифікації переваг особи, що приймає рішення, і передбачає розв'язання підзадач структурного та параметричного синтезу функції загальної корисності $P(q,x)$. У загальному випадку це передбачає вибір критерію подібності, набору інформативних вхідних даних, структури та параметрів функції, оцінки її точності (адекватності до переваг особи, що приймає рішення). За умови визначеної структури моделі $P(q,x)$ задача зводиться до визначення найкращих значень її параметрів з множини допустимих $q \in Q$ [1].

Слід відзначити, що в якості критерію ідентифікації, у залежності від умов функціонування КСКЗ при рішенні задач можна використовувати мінімум сумарної, сумарної квадратичної, максимальної, абсолютної чи відносної похибки оцінки загальної корисності, максимум функції точності вибору тощо [1].

Як зазначено у [1, 7] моделі багатокритеріального оцінювання та вибору синтезуються на основі адитивних, мультиплікативних або змішаних функцій загальної корисності з використанням вагових коефіцієнтів λ_i та функцій корисності $\zeta_i(x)$ часткових критеріїв $k_i(x)$, $i=\overline{1,m}$ [1]. При цьому найбільш поширеною функцією корисності часткових критеріїв є функція:

$$\zeta_i(x)=\left(\frac{k_i(x)-k_i^-}{k_i^+-k_i^-}\right)^{\alpha i}, \qquad (1)$$

де α_i – параметр, що визначає вид залежності (1).

Як вказано в [1], недоліком функції корисності часткових критеріїв (1) вважається її нездатність реалізовувати S- та Z-подібні залежності, що більш адекватно описують ситуації вибору багатокритеріальних рішень з використанням нечіткої математики [9].

З метою врахування групового аргументу та структурно-параметричного синтезу моделей багатокритеріального оцінювання в цих роботах пропонується використання моделі на основі поліному Колмогорова-Габора [1]:

$$P(q,x)=\sum_{i=1}^{m}\lambda_i\zeta_i(x)+\sum_{i=1}^{m}\sum_{j=1}^{m}\lambda_{ij}\zeta_i(x)\zeta_j(x)+...,$$

де m – кількість часткових критеріїв;

λ_i, λ_{ij} – вагові коефіцієнти часткових критеріїв $k_i(x)$ та їх добутків, $\lambda_i \geq 0$, $\lambda_{ij} \geq 0$;

$\zeta_i(x)$ – функція корисності часткових критеріїв;

q – вектор параметрів моделі.

Незважаючи на існуючи переваги цього підходу ідентифікації та широку увагу до нього серед дослідників, ці методи також мають недоліки. Існує декілька причин, що ускладнюють використання цього математичного апарату при вирішенні завдання ідентифікації стану КСКП. Наприклад, однією із таких причин є фіксованість структури

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2019. No. 2 (8)

опорних поліномів, яка обумовлює наступний факт: в процесі самоорганізації опису принципово відсутня можливість синтезу довільного полінома Колмогорова-Габора в процесі еволюційного відбору, породжуються і беруть участь в конкуренції тільки деякі з усіх можливих поліномів.

Формулювання мети статті

Проведений аналіз останніх досліджень і публікацій у напрямі, який розглядається, показав, що актуальним є завдання розробки методів відбору найбільш інформативних показників та синтезу результатів ідентифікаційного вибору а також адаптація до умов функціонування загальної схеми ідентифікації стану КСКП.

Отже метою даної статті є проведення аналізу та розробки загальної схеми синтезу ідентифікаційних вимірів в системі ідентифікації стану комп'ютеризованої системи критичного призначення.

Результати досліджень

Виходячи з даних, отриманих у роботах [4–15] та узагальнюючи результати досліджень можна прийти до висновку, що загальна схема ідентифікації стану КСКП повинна включати до себе методи ідентифікації аномалій та методи ідентифікації зловживань.

Проведені дослідження показали що завдання ідентифікації аномалій в КСКП повинно бути вирішено в умовах дуже складних обмежень на достовірність результатів ідентифікації, причому оперативність вирішення цього завдання не повинно бути гіршим встановлених керівними документами вимог.

Математична формалізація цього завдання полягає у вирішенні оптимізаційної задачі мінімізації ймовірності помилки ідентифікації стану КСКП та виглядає таким чином.

$$P_{пом} \to \min,\ \mathrm{t}_{ід} \le t_{доп},$$

де $P_{пом}$ – ймовірність помилки ідентифікації стану КСКП;

$\mathrm{t}_{ід}$ – час, необхідний для ідентифікації аномалій КСКП;

$t_{доп}$ – допустимий час, необхідний для ідентифікації аномалій КСКП.

Декілька іншою виглядає постановка оптимізаційного завдання при синтезі ідентифікаційних зловживань. У зв'язку з достатньою достовірністю інтелектуальних методів ідентифікації стану існує необхідність мінімізації часу, при встановлених межах ймовірності помилки. Математично цю задачу можна формалізувати наступним чином.

$$\mathrm{t}_{ід} \to \min,\ P_{пом} \le P_{пом\,доп},$$

де $P_{пом\,доп}$ – допустима ймовірність помилки ідентифікації стану КСКП.

В цілому загальну систему ідентифікації стану КСКП можна представити у вигляді схеми, наведеної на рис. 1. На цій схемі наведено таки можливі вхідні дані, що визначені експериментальним шляхом:

X_1 – показник завантаження центрального процесору;

X_2 – показник завантаження оперативної пам'яті;

X_3 – показник кількості операцій запису на диск;

X_4 – показник об'єму переданих/отриманих даних;

X_5 – кількість операцій зчитування з диску;

X_6 – показник завантаження центрального процесору;

X_7 – температура функціонування центрального процесору;

V_1 – швидкість операцій зчитування з диску;

V_2 – швидкість передавання/отримання даних;

V_3, V_4 – сигнатури різних класів шкідливого програмного забезпечення;

V_5 – сигнатури різних видів вторгнень.

Слід зауважити, що основні наукові та практичні результати, отримані за допомогою методів ідентифікації стану на основі BDS-тестування, показника Херста, контрольних карт, дискримінантного та кластерного аналізу, з використанням нейронної мережі, Fuzzi Logic технології та ймовірнісних автоматів наведено у роботах [2–10].

Крім того, у зв'язку з різною характеристикою вихідних параметрів при синтезі ідентифікаційних вимірів аномалії та зловживань, об'єднання цих функцій в одну єдину схему на даний час не представляється можливим. Але і дані окремих ідентифікаційних вимірів стану КСКП, що отримані в схемах ідентифікації аномалій та зловживань, мають практичну цінність при визначені стану технічної системи.

Використовуючи дані та результати досліджень [2–7] проведено порівняльний аналіз розроблених методів ідентифікації аномалій в схемі синтезу ідентифікаційних вимірів КСКЗ. Показниками аналізу в цьому прикладі стали ймовірності хибнонегативної ідентифікації та ймовірності хибнопозитивної ідентифікації. Результати порівняльного аналізу наведено на рис. 2.

Сучасний стан наукових досліджень та технологій в промисловості. 2019. № 2 (8)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

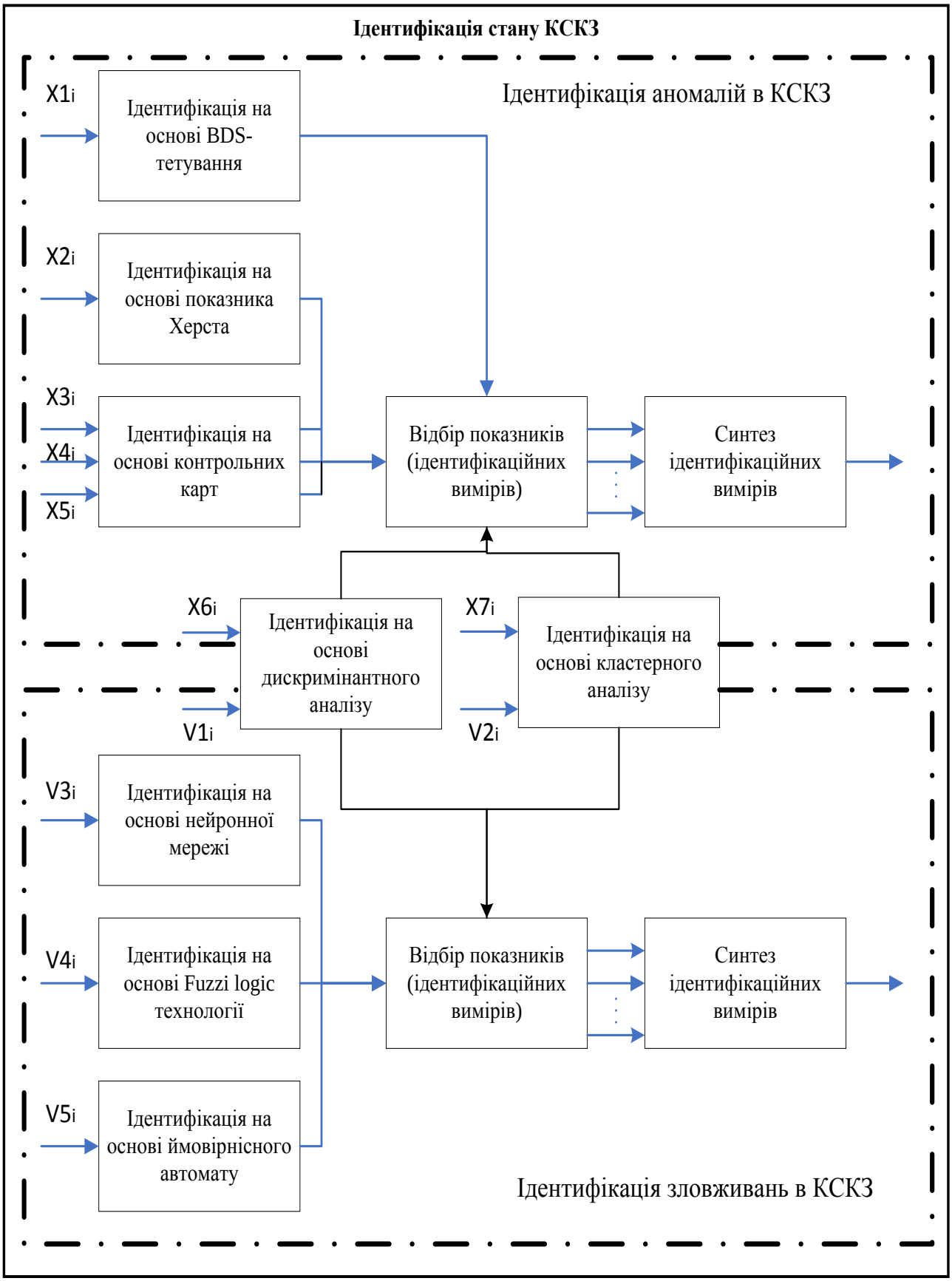

Рис. 1. Загальна система ідентифікації стану КСКП

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2019. No. 2 (8)

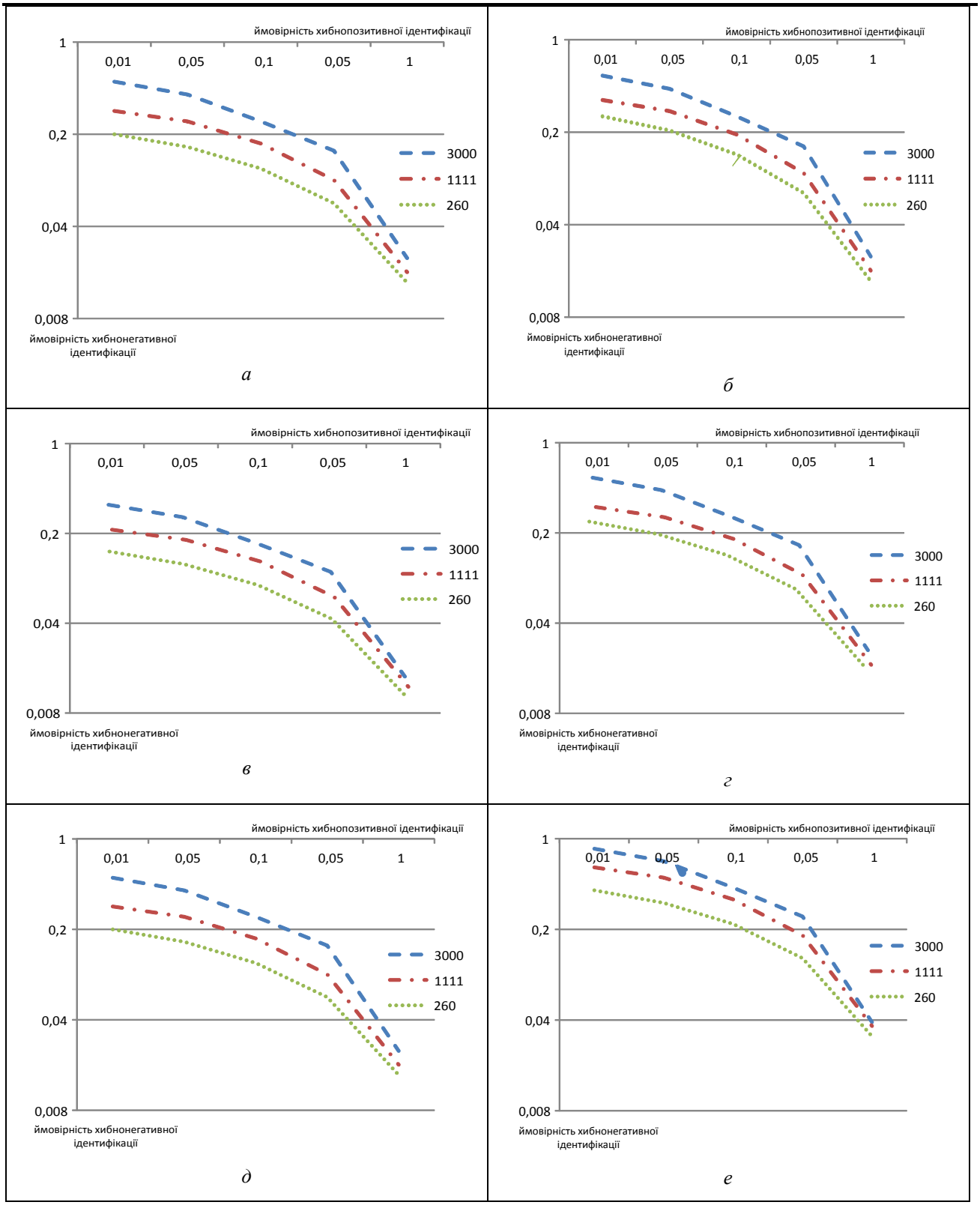

Рис. 2. Результати порівняльного аналізу методів ідентифікації стану

На цьому рисунку графіки 2, а відповідають результатам ідентифікації аномалії з використанням розробленої схеми, а графіки 2, б, в, г, д, е – результатам виконання функції ідентифікації за допомогою BDS-тестування, показника Херста, контрольних карт, дискримінантного та кластерного аналізу відповідно, для реєстрованих даних розміром 3000, 1111, 260.

Як бачимо, комплексне використання методів ідентифікації аномалій КСКП (рис. 1) дозволить підвищити достовірність ідентифікації (знизити ймовірність $P_{пом}$ помилки) до 1,9 разів в порівнянні з звісними методами, або використанням тих же методів, але окремо.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2019. № 2 (8) ISSN 2524-2296 (online)

Проведено порівняльний аналіз розроблених методів ідентифікації зловживань в схемі синтезу ідентифікаційних вимірів КСКЗ. Результати аналізу у вигляді графіків часу ідентифікації в залежності від кількості реєстрованих даних наведено на рис. 3.

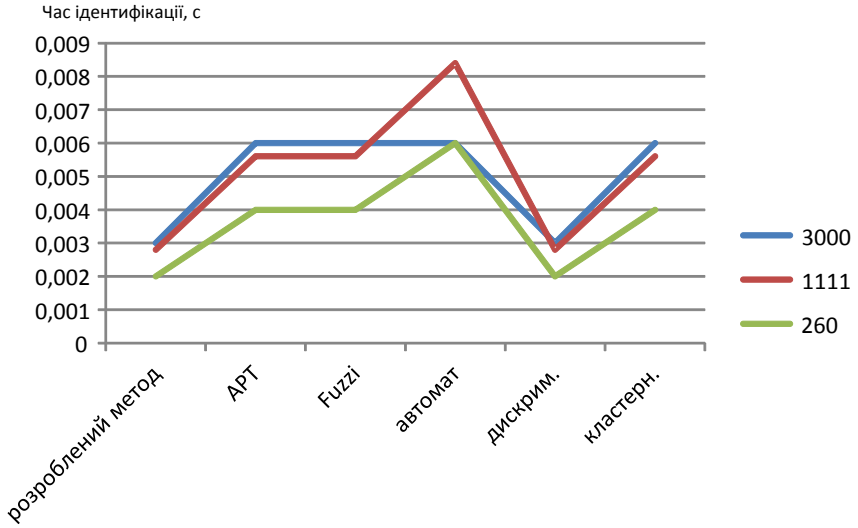

Рис. 3. Графіки часу ідентифікації зловживань КСКЗ в залежності від кількості реєстрованих даних

Як видно з цих графіків комплексне використання методів ідентифікації зловживань в КСКП дозволить підвищити оперативність ідентифікації (знизити час $t_{ід}$) до 2 разів в порівнянні з звісними методами (у тому числі з використанням нейронної мережі).

Висновки

Таким чином, у статті проведено аналіз методів синтезу ідентифікаційних вимірів в комп'ютеризованій системі критичного застосування. Визначено основні перспективні напрямки подальших досліджень. У результаті визначеної класифікації методів ідентифікації стану КСКП сформульовано основні оптимізаційні задачі та наведено приклад можливого використання звісного математичного апарату при їх вирішенні. Це дозволило синтезувати загальну схему ідентифікації стану КСКП, що відрізняється від відомих комплексним використанням вдосконалених методів ідентифікації та їх адаптацією до можливих змін вхідних даних.

Комплексне використання методів ідентифікації аномалій дозволило до 1,9 разів підвищити достовірність ідентифікації, а комплексне використання методів ідентифікації зловживань в КСКП дозволило підвищити оперативність ідентифікації до 2 разів.

Список літератури

1. Безкоровайний В. В., Драз О. М., Семенець В. В. Синтез моделей багатокритеріального оцінювання методом компараторної ідентифікації. Матеріали статей Міжнародної науково-практичної конференції "Інформаційні технології та комп'ютерне моделювання", м. Івано-Франківськ, 14-19 травня 2018 року. Івано-Франківськ : 2018. С. 266–269.
2. Kuchuk, G. A., Kovalenko, A. A., Mozhaev, A. A. (2010), "An Approach To Development Of Complex Metric For Multiservice Network Security Assessment", *Statistical Methods Of Signal and Data Processing (SMSDP – 2010): Proc. Int. Conf., October 13-14, 2010*, Kyiv : NAU, RED, IEEE Ukraine section joint SP, P. 158–160.
3. Гавриленко С. Ю., Горносталь А. А. Разработка адаптивных шаблонов фиксации аномального поведения компьютерной системы. *Системи обробки інформації*. 2016. № 3 (140). С. 11–14.
4. Семенов С. Г., Гавриленко С. Ю., Челак В. В. Разработка шаблонов идентификации состояния компьютерных систем на основе BDS-тестирования. *Вісник НТУ "ХПІ": Інформатика та моделювання*. Харків, 2016. № 21. С. 118–125.
5. Kosenko, V. (2017), "Mathematical model of optimal distribution of applied problems of safety-critical systems over the nodes of the information and telecommunication network", *Advanced Information Systems*, Vol. 1, No. 2, P. 4–9. DOI: https://doi.org/10.20998/2522-9052.2017.2.01
6. Гавриленко С. Ю., Семенов С. Г., Челак В. В. Разработка метода выявления аномального поведения компьютерной системы на основе вероятностного автомата. *Безпека інформації*. Київ, 2018. Т. 24, № 3. С. 163–168. DOI: 10.18372/2225-5036.24.13427
7. Петров К. Э. Компараторная идентификация модели формирования индекса устойчивого развития. *Системні дослідження та інформаційні технології.* 2009. № 1. С. 36–46.
8. Gavrilenko, S., Gavrilenko, S. Yu. (2015), "Formation and study of heuristics in antivirus analyzers using the Mamdani algorithm", *Journal of Qafqaz university, Azerbadhan, Mathematics and computer science*, Vol. 3, No. 3, P. 116–120.
9. Semenov, S., Sira, O, Gavrylenko, S., Kuchuk, N. (2019), "Identification of the state of an object under conditions of fuzzy input data", *Eastern-European Journal of Enterprise Technologies*, Vol. 1, No. 4 (97), P. 22–29. DOI: https://doi.org/10.15587/1729-4061.2019.157085

10. Гавриленко С. Ю., Семенов С. Г., Бабенко А.С. Розробка системи виявлення комп'ютерних вірусів на основі нейронної мережі АРТ-1. *Системи обробки інформації*. Харків : ХУПС, 2015. Вип. 10 (135). С. 126–129.
11. Manikandan, V., Porkodi, V., Amin Salih Mohammed, Sivaram, M. (2018), "Privacy preserving data mining using threshold based fuzzy cmeans clustering", *ICTACT Journal On Soft Computing*, Vol. 09, Issue 01, P. 1813–1816.
12. Semenov, S., Sira, O, Kuchuk, N. (2018), "Development of graphic-analytical models for the software security testing algorithm", *Eastern-European journal of enterprise technologies*. No. 2/4 (92), P. 39–46. DOI: https://doi.org/10.15587/1729-4061.2018.127210
13. Ruban, I., Kuchuk, H., Kovalenko, A. (2017), "Redistribution of base stations load in mobile communication networks", *Innovative Technologies and Scientific Solutions for Industries*, No. 1 (1), P. 75–81. DOI: https://doi.org/10.30837/2522-9818.2017.1.075
14. Коваленко А. А., Кучук Г. А., Рубан И. В. Использование временных шкал при аппроксимации длины очередей компьютерных сетей. *Сучасний стан наукових досліджень та технологій в промисловості*. 2018. № 2 (4). С. 12–18. DOI: http://doi.org/10.30837/2522-9818.2018.4.012
15. Amin Salih Mohammed, Yuvaraj, D., Sivaram Murugan, M., Porkodi, V. (2018), "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, P. 1–6. DOI: http://doi.org/10.26483/ijarcs.v9i6.6335

References

1. Bezkorovayny, V. V., Dras, O. M., Semenec, V. V. (2018), "Synthesis of models of multicriterion estimation by the method of comparative identification" ["Syntez modeley bahatokryterial′noho otsinyuvannya metodom komparatornoyi identyfikatsiyi"], *Materials of the articles of the International scientific and practical conference "Information Technologies and Computer Modeling", Ivano-Frankivsk, May 14-19, 2018*, Ivano-Frankivsk, P. 266–269.
2. Kuchuk, G. A., Kovalenko, A. A., Mozhaev, A. A. (2010), "An Approach To Development Of Complex Metric For Multiservice Network Security Assessment", *Statistical Methods Of Signal and Data Processing (SMSDP – 2010): Proc. Int. Conf., October 13-14, 2010*, Kyiv : NAU, RED, IEEE Ukraine section joint SP, P. 158–160.
3. Gavrilenko, S. Iu., Gornostal, A. A. (2016), "Development the adaptive templates for fixing of the anomalous behavior of the computer system" ["Razrabotka adaptivnykh shablonov fiksatsii anomalnogo povedeniia kompiuternoi sistemy"], *Information Processing Systems*, Vol. 3 (140), P. 11–14.
4. Semenov, S., Gavrilenko, S., Chelack, V. (2016), "Design templates for identification state of computer systems are based on BDS-test", *Herald of the National Technical University "KhPI" : Series "Informatics And Modeling"*, No. 21, P. 118–125. DOI: https://doi.org/10.20998/2411-0558.2016.21.13
5. Kosenko, V. (2017), "Mathematical model of optimal distribution of applied problems of safety-critical systems over the nodes of the information and telecommunication network", *Advanced Information Systems*, Vol. 1, No. 2, P. 4–9. DOI: https://doi.org/10.20998/2522-9052.2017.2.01
6. Gavrilenko, S., Semenov, S., Chelack, V. (2018), "Development of anomalous computer behavior detection method based on probabilistic automaton", *Ukrainian Scientific Journal of Information Security*, Vol. 24, No. 3, P. 163–168. DOI: 10.18372/2225-5036.24.13427
7. Petrov, K. E. (2009), "Comparative identification of the model for the formation of the index of sustainable development" ["Komparatornaya ydentyfykatsyya modely formyrovanyya yndeksa ustoychyvoho razvytyya"], *System research and information technology*, No. 1, P. 36–46.
8. Gavrilenko, S., Gavrilenko, S. Yu. (2015), "Formation and study of heuristics in antivirus analyzers using the Mamdani algorithm", *Journal of Qafqaz university, Azerbadhan, Mathematics and computer science*, Vol. 3, No. 3, P. 116–120.
9. Semenov, S., Sira, O, Gavrylenko, S., Kuchuk, N. (2019), "Identification of the state of an object under conditions of fuzzy input data", *Eastern-European Journal of Enterprise Technologies*, Vol. 1, No. 4 (97), P. 22–29. DOI: https://doi.org/10.15587/1729-4061.2019.157085
10. Semenov, S. H., Havrylenko, S. Yu., Hloba, S. M., Babenko, O. S. (2015), "Development of computer viruses detection system based on ART-1 neural network", *Information Processing Systems*, Vol. 10 (135), P. 126–129.
11. Manikandan, V., Porkodi, V., Amin Salih Mohammed, Sivaram, M. (2018), "Privacy preserving data mining using threshold based fuzzy cmeans clustering", *ICTACT Journal On Soft Computing*, Vol. 09, Issue 01, P. 1813–1816.
12. Semenov, S., Sira, O, Kuchuk, N. (2018), "Development of graphic-analytical models for the software security testing algorithm", *Eastern-European journal of enterprise technologies*. No. 2/4 (92), P. 39–46. DOI: https://doi.org/10.15587/1729-4061.2018.127210
13. Ruban, I., Kuchuk, H., Kovalenko, A. (2017), "Redistribution of base stations load in mobile communication networks", *Innovative Technologies and Scientific Solutions for Industries*, No. 1 (1), P. 75–81. DOI: https://doi.org/10.30837/2522-9818.2017.1.075
14. Kovalenko, A., Kuchuk, H., Ruban, I. (2018), "Using time scales while approximating the length of computer networks", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (4), P. 12–18. DOI: http://doi.org/10.30837/2522-9818.2018.4.012
15. Amin Salih Mohammed, Yuvaraj, D., Sivaram Murugan, M., Porkodi, V. (2018), "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, P. 1–6. DOI: http://doi.org/10.26483/ijarcs.v9i6.6335.

Надійшла (Received) 31.05.2019

Відомості про авторів / Сведения об авторах / About the Authors

Гавриленко Світлана Юріївна – кандидат технічних наук, доцент, Національний технічний університет "Харківський політехнічний інститут", професор кафедри обчислювальна техніка та програмування, Харків, Україна; e-mail: gavrilenko08@gmail.com; ORCID: http://orcid.org/0000-0002-6919-0055.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2019. № 2 (8) *ISSN 2524-2296 (online)*

Гавриленко Светлана Юрьевна – кандидат технических наук, доцент, Национальный технический университет "Харьковский политехнический институт", профессор кафедры вычислительная техника и программирование, Харьков, Украина.

Gavrylenko Svitlana – PhD (Engineering Sciences), Associate Professor, National Technical University "Kharkiv Polytechnic Institute", Professor of the Department of Computer Science and Programming, Kharkiv, Ukraine.

СИНТЕЗ ИДЕНТИФИКАЦИОННЫХ ИЗМЕРЕНИЙ В КОМПЬЮТЕРНОЙ СИСТЕМЕ КРИТИЧЕСКОГО НАЗНАЧЕНИЯ

Предметом исследования являются методы и средства идентификации состояния компьютерной системы критического назначения. **Целью** данной статьи является проведение анализа и разработки общей схемы синтеза идентификационных измерений в системе идентификации состояния компьютерной системы критического назначения. В статье решены следующие **задачи**. Проанализированы методы отбора информативных показателей идентификации состояния и методы синтеза идентификационных измерений в компьютерной системе критического назначения. В результате проведенного анализа сформулированы основные оптимизационные задачи и приведен пример возможного использования известного математического аппарата при их решении. При решении поставленных задач были использованы **методы** многокритериального оценивания, дискриминантного и кластерного анализа, математической статистики и компараторный подход. Полученные **результаты**. Проведенные исследования показали, что общая схема идентификации состояния компьютерной системы критического назначения должна включать методы идентификации аномалий и методы идентификации злоупотреблений, а задача идентификации аномалий в ней должна быть решена в условиях очень сложных ограничений на достоверность результатов идентификации, причем оперативность решения этой задача не должна быть хуже установленных руководящими документами требований. В результате синтезирована общая схема идентификации состояния компьютерной системы критического применения, которая отличается от известных комплексным использованием усовершенствованных методов идентификации и их адаптацией к возможным изменениям входных данных; экспериментальным путем определено множество возможных входных показателей для идентификации состояния; проведен сравнительный анализ методов идентификации состояния; получены графики времени идентификации злоупотреблений в компьютерной системе критического назначения в зависимости от количества регистрируемых данных. **Вывод**: комплексное использование методов идентификации аномалий позволило в 1,9 раза повысить достоверность идентификации, а комплексное использование методов идентификации злоупотреблений в компьютерных системах критического применения позволило повысить оперативность идентификации до двух раз.

Ключевые слова: идентификация состояния; компьютерная система критического применения; идентификационные измерения; идентификация злоупотреблений.

SYNTHESIS OF IDENTIFICATION MEASUREMENTS IN THE COMPUTER SYSTEM OF CRITICAL PURPOSE

The **subject** of the study is the methods and means for identifying the state of a computer system of critical purpose. The **aim** of this article is to conduct an analysis and development of a general scheme for the synthesis of identification measurements in the system of identification of the state of a computer system of critical purpose. The article solves the following **tasks**. The methods of selection of informative indicators of state identification and methods for the synthesis of identification measurements in a computer system of critical purpose are analyzed. As a result of the analysis, the main optimization problems are formulated and an example of the possible use of the known mathematical device in their solution is given. When solving the tasks, **methods** of multi-criteria evaluation, discriminant and cluster analysis, mathematical statistics and comparative approach were used. **Results** obtained. Studies have shown that the general scheme for identifying the state of a computer system of critical purpose should include methods for identifying abnormalities and methods for identifying abuses. The task of identifying anomalies should be solved under very difficult constraints on the authenticity of the results of identification, and the efficiency of the solution to this problem should be worse than the requirements set forth in the guideline documents. As a result, a general scheme for identifying the state of a computer system of critical purpose that differs by the complex use of advanced identification methods and their adaptation to possible changes in input data is synthesized. The set of possible input indicators for state identification was experimentally determined. A comparative analysis of state identification methods was conducted. The timetables for identifying abuses in a computer system of critical purpose, depending on the number of recorded data were received. **Conclusion**: the complex use of the methods of identification of anomalies allowed to increase the authenticity of identification to 1,9 times, and the complex use of methods for identifying abuses in computer systems of the critical purpose allowed to increase the efficiency of identification up to 2 times.

Keywords: state identification; computer system of critical purpose; identification dimensions; identification of abuses.

Бібліографічні описи / Bibliographic descriptions

Гавриленко С. Ю. Синтез ідентифікаційних вимірів в комп'ютерній системі критичного призначення. *Сучасний стан наукових досліджень та технологій в промисловості*. 2019. № 2 (8). С. 36–43. DOI: https://doi.org/10.30837/2522-9818.2019.8.036.

Gavrylenko, S. (2019), "Synthesis of identification measurements in the computer system of critical purpose", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (8), P. 36–43. DOI: https://doi.org/10.30837/2522-9818.2019.8.036.