

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0519U001849

Особливі позначки: відкрита

Дата реєстрації: 11-12-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Гавриленко Світлана Юріївна

2. Gavrylenko Svitlana

Кваліфікація: к. т. н., 05.17.08

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 05-12-2019

Спеціальність за освітою: Автоматика і телемеханіка

Місце роботи здобувача: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, 2, м. Харків, Харківський р-н., Харківська обл., 61002, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 64.050.14

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, 2, м. Харків, Харківський р-н., Харківська обл., 61002, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, 2, м. Харків, Харківський р-н., Харківська обл., 61002, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи та засоби ідентифікації стану комп'ютерних систем критичного застосування для захисту інформації
2. Methods and means of identification of computer systems of critical application state for information protection

Реферат:

1. Дисертацію присвячено підвищенню оперативності та достовірності ідентифікації стану комп'ютерних систем критичного застосування шляхом розробки та удосконалення методів та засобів розпізнавання аномалій та зловживань. Проведено аналіз науково-технічної проблеми ідентифікації стану КСКЗ для захисту даних. Виконано порівняльні дослідження існуючих методів та відомих комп'ютеризованих систем ідентифікації стану, виявлено ряд обмежень їх використання. Зроблено висновок про перспективність напрямку розробки та дослідження комплексних методів ідентифікації стану КСКЗ. Розроблено схему ідентифікації стану КСКЗ, яка включає підсистему ідентифікації аномалій та зловживань. Синтезовано критерії оцінки інформативності показників функціонування КСКЗ. Виконано модернізацію методу дискримінантного і кластерного аналізу за умови нечітких вихідних даних. Розроблено експертну систему з

непродукційним механізмом логічного виведення, що дозволило виконати ідентифікацію стану КСКЗ з необмеженим числом контрольованих показників. Розроблено експрес-метод ідентифікації стану КСКЗ на основі комплексного використання статистичних методів класифікації, що включає BDS-тестування, оцінку показників Херста та контрольних карт Шухарта, CUSUM та EWMA, що дозволило збільшити достовірність ідентифікації вторгнень в КСКЗ. Синтезовано новий показник нормального функціонування КСКЗ, на основі BDS-статистики, який відрізняється від відомих використанням синтезованого показника джиттера параметрів системи. Удосконалено метод ідентифікації стану КСКЗ на основі комплексного використання інтелектуальних методів ідентифікації, що включає нейронну мережу АРТ-1, систему нечіткого виведення Мамдані та ймовірнісний автомат, що підвищило оперативність ідентифікації вторгнень в КСКЗ. Виконано порівняльне дослідження та оцінку достовірності та оперативності розроблених методів та засобів ідентифікації аномалій та зловживань в КСКЗ, надано практичні рекомендації

2. The thesis is dedicated to the enhancement of efficiency and reliability of the identification of the computer systems of critical application state by means of development and improvement of methods and means of recognition of anomalies and abuses. A scheme of the identification of the CSCA state that includes the subsystem of the anomaly and abuse identification was proposed. The basis of performance of the abuse identification subsystem is complex use of intelligent classification methods that includes the neural network ART-1, the improved models of fuzzy output and the probabilistic automaton. Complex use of the statistical methods of classification and the decision support systems based on discriminant, cluster and Bayes classifiers. Enhancement of the discriminant analysis method under the condition of fuzzy input data was performed for the two-alternative classification. It was based on the analogies of theoretic and probabilistic characteristics of fuzzy numbers, particularly, the expected value, the dispersion of correlation coefficients, used for the standard calculation scheme by means of the solution of the linear equation system and the classification of the object state. In the present work the enhancement of the cluster analysis under condition of fuzzy specification of the point coordinates (the results of measurements of controlled parameters) and the centers of cluster groups, defined by membership functions, was done for the multi-alternative diagnostic. The procedure of the comparison of fuzzy distances between the objects of clustering and the group centers, based on the comparison of fuzzy function of distance difference with zero was proposed. The rules for the result treatment of the comparison of fuzzy number with zero were developed. A criterium of self-descriptiveness estimation of the performance parameters of CSCA under fuzzy input data, the value of which belongs to the final range, does not depend on the parameter membership function type and on the rules of inclusion of the function into evaluation expression, was found. The self-descriptiveness rate of the controlled fuzzy parameters, described by gaussian, exponential functions of membership and the criterium based on the surface evaluation of the area of intersection of the state membership functions was developed. An expert system with non-productional mechanism of logic inference based on modified Bayes classifier was created for identification of the CSCA state with infinite numbers of controlled parameters. An express method of identification of the CSCA state relied on complex use of statistic methods of classification including BDS test, the evaluation of Hurst exponent and Shewhart charts, CUSUM and EWMA, as components of the subsystem on anomaly recognition, was worked out. A new parameter of normal performance of CSCA based on the jitter value of the system was synthesized and a template of normal behavior of CSCA arising from BDS test and Hurst exponent values was proposed. The templates of the normal system state of CSCA relying on Shewhart charts, CUSUM and EWMA were built. A classification method of CSCA state based on the neuron network ART-1 that included complex use of ART-1 blocks was developed. The use of the proposed method improved the efficiency of identification of the CSCA state. A method of identification of the CSCA state relying on the system of fuzzy output, which differs from the well-known by the use of minimization procedure of number of rules linking input and output fuzzy variables, was suggested. It allowed to improve efficiency of the identification of CSCA state. On the basis of ROC-analysis a comparative study and an estimation of reliability and efficiency of developed methods and means of anomaly and abuse identification in CSCA was performed. Practical recommendations on the use of the methods and means of the anomaly and abuse identification of the CSCA were proposed.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Семенов Сергій Геннадійович

2. Semenov Serhii H.

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Семенов Сергій Геннадійович

2. Semenov Serhii H.

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Єременко Володимир Станіславович
2. Yeremenko Volodymir Stanislavovich

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Кривуля Геннадій Федорович
2. Kryvulia Hennadii F.

Кваліфікація: д. т. н., 05.13.00

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Чемерис Олександр Анатолійович
2. Chemerys Oleksandr A.

Кваліфікація: д. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові
голови ради**

Качанов Петро Олексійович

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Качанов Петро Олексійович

**Відповідальний за підготовку
облікових документів**

Реєстратор

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Т.А.