Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0419U000516

Особливі позначки: відкрита

Дата реєстрації: 26-02-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Балакін Сергій В'ячеславович
2. Balakin Sergiy Vyacheslavovich

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

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: 14-02-2019

Спеціальність за освітою: Комп'ютерні системи та мережі

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.062.07

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київська обл., 03058, 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 авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київська обл., 03058, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.55.01

Тема дисертації:

1. Методи та засоби підвищення достовірності ідентифікації несанкціонованих дій та атак в комп'ютерній мережі

2. Methods and ways of increasing the reliability of the identification of unauthorized actions and attacks in the computer network

Реферат:

1. Дисертаційну роботу присвячено вирішенню актуального науково-технічного завдання – підвищенню достовірності ідентифікації несанкціонованих дій і атак в комп’ютерній мережі. Для ефективної, надійної та високошвидкісної ідентифікації несанкціонованих дій і атак в комп’ютерній мережі потрібно впроваджувати і використовувати методи, основані як на штучних імунних системах, так і на можливості діагностування вторгнень. Такий підхід дозволить підвищити ефективність ідентифікації несанкціонованих дій і дасть можливість автономно виявляти підозрілу активність. У роботі визначено методи виявлення несанкціонованих дій і атак в комп’ютерній мережі за рахунок використання засобів штучних імунних систем та діагностування на основі теорії Демпстера-Шафера, котрі дають можливості ефективно протидіяти вторгненням. Досліджено можливості використання операторів імунних систем для моделювання роботи запропонованих методів. На основі цих властивостей запропоновано процедури ідентифікації

несанкціонованих дій і атак в комп'ютерній мережі. Сформульовано необхідні критерії та вимоги для забезпечення своєчасного виявлення вторгнень у комп'ютерні мережі. Визначено основні напрями розвитку сучасних методів аналізу вторгнень і можливості автономного виявлення НД. Аналіз сучасних вторгнень показав доцільність розроблення методів, котрі дадуть змогу виявляти як відомі, так і нові НД. Проведено порівняльний аналіз моделей і методів, які можливо використовувати при розпізнаванні НД в комп'ютерній мережі. Порівняно характеристики методів і вказано на їх сильні та слабкі сторони. Сформовано вимоги до вибраних методів на основі збереження швидкодії та можливості автономного виявлення НД (без використання і звернення до сигнатурних баз даних). Розглянуто методи штучних імунних систем, котрі дають змогу підтримувати автономне виявлення нових НД при високій швидкості обробки інформації та адаптивності. Виявлення НД за допомогою діагностування дає можливість розширити спектр потенціальних вторгнень за допомогою використання операторів ТДШ. При поєднанні різних технологій при використанні методів ТДШ можливо досягнути високої швидкості та надійності виявлення НД в комп'ютерних мережах. Проведено дослідження ефективності методу виявлення НД в комп'ютерній мережі на основі штучних імунних систем і діагностування. На основі аналізу отриманої інформації зроблений наступний висновок: при коректній навчальній вибірці та вірному виборі параметрів навчання метод ШІМ має однаково високу достовірність виявлення нових НД як і метод діагностування. ШІМ потребує додаткового часу на утворення навчальної вибірки, але це дозволяє системі швидше реагувати на нові види НД і знизити кількість помилкових спрацювань. Метод діагностування менше навантажує систему користувача, але частіше визначає підозрілу активність як НД. Результати порівняльного аналізу НД показують, що запропоновані методи перевершують відомі антивірусні продукти, використані в порівняльному тесті та здатні виявити невідомі НД. Теоретично та експериментально доведено ефективність запропонованих методів. Результати теоретичних та експериментальних досліджень упроваджено у виробництво та навчальний процес.

2. The thesis is devoted to solving the actual scientific and technical problem - increasing the reliability of identification of unauthorized actions and attacks in the computer network. For effective, reliable and high-speed identification of unauthorized actions and attacks in a computer network, methods should be implemented and used based on both artificial immune systems and the ability to diagnose intrusions. Such an approach will increase the effectiveness of identifying unauthorized actions and will provide an opportunity to autonomously detect suspicious activity. The work defines methods for detecting unauthorized actions and attacks in a computer network through the use of artificial immune systems and diagnostics based on the Dempster-Shafer theory, which makes it possible to effectively detect intrusions. The possibilities of using the operators of immune systems for modeling the work of the proposed methods are explored. Based on these properties, procedures are proposed for identifying unauthorized actions and attacks in a computer network. The necessary criteria and requirements are formulated for ensuring timely detection of intrusions in computer networks. The basic directions of development of modern methods of analysis of intrusions and possibilities of autonomous detection of intrusions are determined. An analysis of modern intrusions has shown the feasibility of developing methods that will be able to detect both known and new intrusions. A comparative analysis of models and methods that can be used for intrusion recognition in a computer network is carried out. The comparative characteristics of the methods are indicated on their strengths and weaknesses. The requirements for the selected methods are formed on the basis of maintaining the speed and the ability to independently identify the intrusion (without the use and access to signature databases). Detection of intrusions by means of diagnostics enables to expand the spectrum of potential intrusions by using Dempster-Shafer operators. When combining different technologies with the use of Dempster-Shafer methods it is possible to achieve high speed and reliability of detection of intrusions in computer networks. The research of the effectiveness of the method of detection of intrusions in a computer network on the basis of AIS and diagnostics was carried out. On the basis of the analysis of the information obtained, the following conclusion was made: with a correct training sample and a correct choice of learning parameters, the AIS method has the same high reliability as the diagnostic method. AIS requires additional time to create a training sample, but this allows the system to respond more quickly to new types of intrusions and reduce the number of false positives. The diagnostic method is less burdensome for the user system, but more often it identifies suspicious

activity as intrusion. The results of the comparative analysis of intrusions show that the proposed methods outperform the known antiviral products used in the comparative test and are capable of detecting unknown intrusions. Proved the effectiveness of proposed methods. The results of theoretical and experimental research are introduced into the production and educational process.

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. Жуков Ігор Анатолійович
2. Zhukov Igor A.

Кваліфікація: д. т. н., 05.13.13

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. Чемерис Олександр Анатолійович
2. Chemerys Oleksandr Anatolijovych

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. Галелюка Ігор Богданович
2. Galelyuka Igor Bogdanovyxh

Кваліфікація: к. т. н., 05.13.06

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	Жуков Ігор Анатолійович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Печурін Микола Капітонович
Відповідальний за підготовку облікових документів	
Реєстратор	

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.