Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0415U003841

Особливі позначки: відкрита

Дата реєстрації: 03-07-2015

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Мамарєв Віктор Миколайович
2. Mamarev Victor

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 21.05.01

Назва наукової спеціальності: Інформаційна безпека держави

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 30-06-2015

Спеціальність за освітою: 7.090781

Місце роботи здобувача: Національний центр управління та випробувань космічних засобів Державного космічного агентства України

Код за ЄДРПОУ: 24507442

Місцезнаходження: 01010, Київ, вул. Московська, 8.

Форма власності:

Сфера управління: Національне космічне агенство України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): К 26.861.06

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

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

Повне найменування юридичної особи: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: 03680 Україна, м. Київ, вул. Солом'янська, 7

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. Метод побудови класифікатора кібератак на державні інформаційні ресурси

2. Method of constructing classifier of cyber attacks on governmental information resources

Реферат/анотація:

1. Об'єкт дослідження: процеси виявлення і класифікації кібератак (КБа) на державні інформаційні ресурси (ДІР). Метою дослідження є підвищення рівня захищеності ДІР шляхом розробки методу побудови класифікатора КБа, що забезпечує функціонування СІБ ДІР в масштабі часу, наближеному до реального. Методи дослідження: методи теорії ймовірностей, теорії інформації, теорії багатокритерійної оптимізації, методи і алгоритми інтелектуального аналізу даних. Наукова новизна: вперше розроблено метод оцінювання інформативності та селекції дуетів станів ІКС, в основу якого покладено процедуру оцінювання зваженого приросту інформації параметрів потоків вхідних даних (ПВхД) систем інформаційної безпеки (СІБ) ДІР, що дозволяє забезпечити селекцію останніх за критерієм максимальної віддаленості у просторі параметрів; вперше розроблено метод скорочення розмірності ПВхД для СІБ ДІР, в основу якого покладено метод вкладених скалярних згорток, що дозволяє, не погіршуючи показників точності класифікації КБа, оперативніше реалізовувати процедури скорочення розмірності ПВхД класифікаторів; удосконалено метод побудови класифікатора КБа на ДІР, який відрізняється від відомих процедурою побудови останнього у

вигляді двоетапного бінарного класифікатора на базі дерев рішень та скорочених ПВхД, що дозволяє підвищувати оперативність виявлення і класифікації станів ІКС при одночасному забезпеченні заданих показників захищеності ДІР. Практичне значення одержаних результатів у сукупності складає підґрунтя для вдосконалення класифікаторів КБа на ДІР та забезпечує функціонування СІБ ДІР в масштабі часу, наближеному до реального.

2. The object of research: the processes of cyber attacks on governmental information resources detection and classification. The goal of research is to increase the level of protection of state information resources through the development of methods of constructing the classifier of cyber attacks on governmental information resources, ensuring operation of the information security system of the governmental information resources in a scale near to real time. For the first time a assessment method for information content parameters and selection governmental network status duets was elaborated, which is based on information content assessment of binary duets parameters of event patterns - templates of normal system behavior of the system and patterns of attacks, as well as attacks templates' class duets that allowed to perform duets selection of the last mentioned classes under the criteria of maximum distance in the parameter space. For the first time a method for dimension reduce of input data streams was elaborated for the information security system of governmental information resources, which is based on using a method of inserted scalar convolutions which allowed faster implement reduce procedure for streams dimension of input data classifiers not compromising the performance of classification accuracy of cyber attacks. The method of constructing the cyber attacks classifier on governmental information resources was improved, which differed from the known ones by procedure of constructing the cyber attacks classifier in the form of a two-stage binary classifier based on decision trees and reduced input data flows, which allowed increase of the efficiency of detection and classification of condition of the information and telecommunication systems along with synchronous provision of specified protection indexes of the governmental information resources.

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. Бурячок Володимир Леонідович

2. Buryachok Volodymyr

Кваліфікація: д.т.н., 21.05.01

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. Пархуць Любомир Теодорович
2. Пархуць Любомир Теодорович

Кваліфікація: д.т.н., 05.13.21

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. Гнатюк Сергій Олександрович
2. Гнатюк Сергій Олександрович

Кваліфікація: к.т.н., 05.13.21

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	Бурячок Володимр Леонідович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Бурячок Володимр Леонідович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.

