Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U002495

Особливі позначки: відкрита

Дата реєстрації: 24-04-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Корченко Анна Олександрівна
2. Korchenko Anna Oleksandrivna

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: 23-04-2013

Спеціальність за освітою: 8.160102

Місце роботи здобувача: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

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): К 26.820.04

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: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: 03058,Україна,м.Київ,Просп.Космонавта Комарова,1

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. Моделі аномального стану для систем виявлення кібератак в комп'ютерних мережах

2. The models of anomaly-based cyberattacks detection system in computer networks

Реферат:

1. Дисертаційна робота присвячена вирішенню актуальної наукової задачі розробки моделей та засобів ідентифікації аномального стану для розширення можливостей системи виявлення несигнатурних типів кібератак в комп'ютерних мережах. Застосування математичного апарату теорії нечітких множин для побудови засобів виявлення аномалій, породжених атакуючими діями, дозволить удосконалити існуючі системи виявлення вторгнень. Розроблена базова модель параметрів та універсальна модель еталонів, що дозволяють формалізувати процес побудови еталонних значень та встановлювати відповідність між типом атаки і необхідними для її ідентифікації атрибутами. Побудована модель евристичних правил, яка за рахунок множини еталонних параметрів, логіко-лінгвістичних зв'язок та лінгвістичних ідентифікаторів, дозволяє формалізувати процес формування множин евристичних правил для виявлення аномального стану. Розроблено метод виявлення аномалій, який за рахунок зазначених моделей і сформованих поточних параметрів, дозволяє будувати засоби виявлення несигнатурних та нових типів кібератак. На основі методу запропоновані нові структурні рішення для удосконалення систем мережевої безпеки та розроблено

алгоритмічне і програмне забезпечення для виявлення аномального стану, яке може застосовуватись автономно або як розширювач функціональності сучасних систем виявлення вторгнень. Всі результати, що отримані експериментальним шляхом за допомогою практичного використання програмних розробок співпадають з теоретичними та підтверджують їх. Основні результати впроваджено в діяльність в/ч К-1410, Інституту кібернетики імені В.М. Глушкова НАН України, Національного авіаційного університету та Черкаського державного технологічного університету.

2. The dissertation deals with the scientific problem-solving approach of the models development and identification methods of anomalous condition to increase the possibilities of non-signature types of cyber attack detection system in computer networks. It was developed the basic model of parameters and the universal model of linguistic variables standards, that admit to formalize the process of reference values and set the correspondence between the type of attack and necessary for its identification attributes. The designed heuristic model, which is due to a set of reference parameters, logical-linguistic links and language IDs makes possible to formalize the process of heuristic rules formation for the abnormal condition detection. This paper investigates the anomaly detection technique, which due to the mentioned models and current settings was developed for creating the non-signature and new types of cyber attacks detection techniques. On the basis of the method there were proposed some new structural solutions for network security improvement and also were developed the algorithmic support and software for abnormal condition detection, which can be used standalone or as the extender functionality of modern intrusion detection systems. All the results obtained experimentally with the practical use of software development coincide with theoretical and confirm them. The main results were adopted by the VM Glushkov Institute of Cybernetics of NAS of Ukraine, The National Aviation University and Cherkasy State Technological University.

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. Стасюк Олександр Іонович

2. Stasiuk Alexander Ionovich

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. Лужецький Володимир Андрійович

2. Лужецький Володимир Андрійович

Кваліфікація: д.т.н., 01.05.02, 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. Гільгурт Сергій Якович

2. Гільгурт Сергій Якович

Кваліфікація: к.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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Стасюк Олександр Іонович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Стасюк Олександр Іонович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.