Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0519U000618

Особливі позначки: відкрита

Дата реєстрації: 15-07-2019

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Корченко Анна Олександрівна
2. Korchenko Anna O.

Кваліфікація: к. т. н., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 02-07-2019

Спеціальність за освітою: 8.160102 Захист інформації з обмеженим доступом та автоматизація її обробки

Місце роботи здобувача: 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

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.062.17

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: 20.56.02

Тема дисертації:

1. Методи ідентифікації аномальних станів для систем виявлення вторгнень
2. Methods for identifying abnormal states for intrusion detection systems

Реферат:

1. Дисертаційна робота присвячена вирішенню актуальної науково-прикладної проблеми, яка пов'язана з розробкою методів ідентифікації аномальних станів для систем виявлення вторгнень (СВВ). В роботі проведено аналіз сучасних СВВ відносно базових характеристик, як-от «Клас кібератак», «Адаптивність», «Відкритість», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» та «Підтримка ОС». Це надає можливості розробникам і користувачам обирати необхідні методи та відповідне програмне забезпечення (ПЗ) для захисту інформаційних систем (ІС) і будувати відповідні системи безпеки. На основі цього, розроблено кортежну модель формування атакуючих середовищ, яка дозволяє сформувати набір часткових кортежів, для симуляції процесу виявлення аномального стану в m-вимірному гетерогенному параметричному середовищі, утвореного відповідним атакуючим середовищем у заданий часовий проміжок. Також розроблений метод формування еталонів, для формалізації процесу отримання еталонних середовищ, які містять множини значень фіксованих параметрів заданих груп лінгвістичних змінних, що характеризують

конкретне еталонне підсередовище. Запропоновані методи фазифікації та дефазифікації параметрів, які дозволили формалізувати процес перетворення значень параметрів m-вимірних поточних середовищ для їх подальшого застосування у виявленні аномального стану та відобразити параметри детекційного середоваща, що характеризують у числовій формі рівень упевненості експерта відносно його суджень щодо можливих кібератак. Розроблений метод □-рівневої номіналізації нечітких чисел, який дозволив здійснити графічну інтерпретацію нечітких величин та визначення ідентифікуючих термів, що відображають у заданий момент часу значення еталонних та поточних підсередовищ, які характерні для реалізації певних типів кібератак на ресурси ІС. Запропонований метод визначення ідентифікуючих термів, для пошуку в заданих лінгвістичних змінних, ідентифікуючих перетворених еталонних термів, за якими за допомогою детекційних виразів, визначаються рівні аномальних станів. Розроблений метод формування детекційного середовища для побудови необхідної множини детекційних правил, що використовуються при визначенні поточного рівня аномального стану, характерного дії визначеного типу кібератак в m-вимірному гетерогенному параметричному середовищі. На підставі запропонованих методів і моделі розроблено методологію побудови систем виявлення аномалій, породжених кібератаками, яка використовується для визначення рівня аномального стану в m-вимірному гетерогенному параметричному середовищі. Розроблено структурне рішення обчислювальної системи виявлення кібератак, що дозволяє за допомогою визначення рівня аномального стану, характерного впливу певного типу кібератак, розширити функціональні можливості сучасних СВВ. Також, на базі запропонованої методології та відповідного структурного рішення розроблено алгоритмічне забезпечення та програмна модель системи, яка може використовуватися автономно або бути розширювачем функціональних можливостей сучасних СВВ. Проведені експериментальні дослідження підтвердили достовірність теоретичних положень та практичних розробок дисертаційного дослідження.

2. The functionality of modern intrusion detection and blocking systems depends to a great extent on their capabilities to detect new cyberattacks in real time. Systems for countering cyberattacks are well developed, but their effective operation requires appropriate information that is supposed to be helpful in detecting attack actions. As a rule, such data is formed post facto and requires certain time. So, detection and blocking of new cyberattacks are characterized by the conflict between the readiness of cyberattack counteraction systems to immediately respond to an intrusion and the lack of readiness of detection tools to appropriately inform the counteraction functional. In order to deal with this problem, it is necessary to design specific tools that would enable enlarged functional capabilities of modern intrusion detection systems through the a priori formation of information about anomalous states in information systems caused by certain cyberattack types. For this purpose, the most effective approach consists in using the expert knowledge, which, as a rule, is represented in the form of the expert's judgments about the parameters abnormality level caused by the effect of new types of threats. The dissertation deals with a pressing applied scientific problem related to detection of new kinds of cyberattacks within the shortest possible time by designing an appropriate methodology of creating systems for detecting anomalous states caused by new types of threats. The methodology is supposed to focus on creation of tools that would enlarge the functionality of modern intrusion detection systems. Also, on the basis of the proposed methodology and the corresponding structural solution, an algorithmic support and a software model of a system for detecting anomalous states created by cyberattacks are designed. The model can be used either autonomously or to expand the functionality of modern intrusion detection systems. The conducted experiments confirmed the reliability of the theoretical principles and practical developments of the dissertation. The results of the study have been adopted by the Saifer BIS Ltd Company. They are also used in the educational process at the Department of Data Protection Computerized Systems of the National Aviation University, at the Information Security Department of the Institute of Information and Telecommunications Technologies of K.I. Satbayev Kazakh National Research Technical University and at the Department of Computer Science and Automatics of the University (Technical-Humanistic Academy) of Bielsko-Biała, Poland.

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. Терейковський Ігор Анатолійович
2. Tereykovskyy Ihor A.

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. Терейковський Ігор Анатолійович
2. Tereykovskyy Ihor A.

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Опірський Іван Романович
2. Opirskyy Ivan R.

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. Лужецький Володимир Андрійович
2. Luzhetsky Volodymir 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

Власне Прізвище Ім'я По-батькові:

1. Грищук Руслан Валентинович
2. Hryshchuk Ruslan V.

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Щербак Леонід Миколайович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Щербак Леонід Миколайович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.