Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0417U003325

Особливі позначки: відкрита

Дата реєстрації: 29-06-2017

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Гнатюк Віктор Олександрович

2. Gnatyuk Viktor

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат 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: 27-06-2017

Спеціальність за освітою: 8.03050201

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): 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: 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. Методи обробки кіберінцидентів в інформаційно-телекомунікаційних системах

2. Methods for Cyberincidents Processing in Information & Telecommunication Systems

Реферат/анотація:

1. Дисертаційна робота присвячена розв'язанню актуальної науково-практичної задачі розробки і дослідження нових ефективних методів обробки КбІ в ІТС протягом всього їх життєвого циклу для розширення функціональних можливостей центрів реагування на КбІ CSIRT. У роботі розроблено метод категоризації КбІ для підвищення ефективності реагування на них. Також розроблено ПЗ для категоризації КбІ, який може використовуватись як автономний інструментальний засіб CSIRT, або у якості модуля системи SIEM (у контексті агрегації даних, їх кореляції та експертного аналізу) для категоризації КбІ. Крім того, розроблено практичні рекомендації щодо застосування оперативних контрзаходів для локалізації КбА / КбІ різних категорій. Розроблено метод оцінювання ефективності обробки КбІ центрами CSIRT для аудиту їх діяльності. Також розроблено систему базових показників, які можуть використовуватися для оцінювання ефективності обробки КбІ центрами CSIRT та іншими центрами технічного обслуговування ІТС. Розроблено концепцію та метод МЦ моніторингу КбІ, що дозволяє визначити найбільш важливі об'єкти захисту, прогнозувати категорії КбІ, які виникнуть внаслідок реалізації КбА, та їх рівень небезпеки. Розроблено також і

відповідне ПЗ, що може використовуватися для моніторингу КбІ та їх впливу на складові ІТС шляхом аналізу статистичних даних CSIRT та підключення до баз КбА KDD 99, CAPEC та ін. Розроблено метод формування множини правил екстраполяції КбІ, який дозволяє автоматизувати і підвищити точність роботи систем МЦ моніторингу ІТС.

2. Thesis is devoted to applied scientific research task to develop and study new effective methods for cyberincidents processing in information & telecommunication systems during its life cycle for extending CSIRT (Computer Security Incident Response Team) functional possibilities from viewpoint of cyberincidents response. In the thesis modern approaches to cyberincidents processing in information & telecommunication systems was analyzed using multicriteriality. As follows from the analysis the disadvantages of existing methods, models and systems were defined. These issues disagree to international standards requirements of incident-management particularly ISO 27035, ITIL, NIST 800-61, ITU-T E.409 and don't give possibility to implement procedures of cyberincidents detection, categorization, monitoring and prediction in information & telecommunication systems and also to realize CSIRT audit. Method for cyberincidents categorization was developed using plain data processing by misuse and anomaly detection, Big Data specialized procedures, entropy decreasing (information amplifying) and categorization quality metrics calculation. This method allows to define cyberincidents categories in information & telecommunication systems more accurate and provide E2 and E3 phases of cyberincident life cycle in accordance to ITU-T E.409. Also software for cyberincidents categorization was developed and this can be used as both autonomous CSIRT tool and also SIEM module (from viewpoint of data aggregation, correlation and expert analysis) to categorize cyberincidents with accuracy of 99.96% (for some cyberincidents categories). Besides practical guidelines for response and counteraction implementation was created to localize different categories of cyberattacks / cyberincidents. Method for CSIRT efficiency assessment in context of cyberincidents processing was developed. It gives possibility to realize CSIRT (and also others technical support centers for information & telecommunication systems) audit and provide H2.2 phase of cyberincident life cycle in accordance to ITU-T E.409. This method uses parameters (indicators) defining, key performance indicators identifying by multifactor correlation and regression analysis, indicator panel creation, KPI / E visualization. Also the system of basic indicators was developed and can be used for CSIRT and others technical support centers like Service Desk, Help Desk etc. The concept and method for network centric cyberincidents monitoring, it uses cyberattacks classification, parameters comparison with standards, basic extrapolation rules forming, cyberattack classes and cyberincident categories communication based on statistics, security objects identifying and cyberincidents criticality ranking. It gives possibility to define most critical security objects (components of information & telecommunication systems or cybersecurity segments), to predict cyberincidents categories and its criticality level and also provide H1 and H2 phases of cyberincident life cycle in accordance to ITU-T E.409. Also software for cyberincidents monitoring using statistical data and connection to KDD 99, CAPEC bases was developed. Method for set of cyberincidents extrapolation rules forming was developed and it defines cyberattacks types and cyberincidents categories, forms cyberincidents realization probability matrixes, make cyberincidents ranking and indicators of cyberincidents appearance. This method allows to automate network centric cyberincidents monitoring with high accuracy level provide E5.1 phase of cyberincident life cycle in accordance to ITU-T E.409. Also the system of basic rules was developed and it can be used for cyberincidents identifying based on cyberattack statistics.

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. Іванченко Євгенія Вікторівна
2. Ivanchenko Yevgeniya

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. Смірнов Олексій Анатолійович

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

Власне Прізвище Ім'я По-батькові:

1. Опірський Іван Романович

2. Опірський Іван Романович

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 Корченко Олександр Григорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Корченко Олександр Григорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.