Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0521U100109

Особливі позначки: відкрита

Дата реєстрації: 02-02-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Радівілова Тамара Анатоліївна

2. Radivilova Tamara

Кваліфікація: к. т. н., 01.05.02

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

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: 28-01-2021

Спеціальність за освітою: Захист інформації в комп'ютерних системах

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, буд. 14, м. Харків, Харківський р-н., Харківська обл., 61166, 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 26.861.06

Повне найменування юридичної особи: Державний університет телекомунікацій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, м. Київ, Київська обл., 03680, 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: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, буд. 14, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

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 та методи забезпечення безпеки та якості обслуговування в комп'ютерних системах із самоподібними інформаційними потоками

2. Models and methods of ensuring security and quality of service in computer systems with self-similar information flows

Реферат/анотація:

1. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». – Харківський національний університет радіоелектроніки. – Державний університет телекомунікацій, м. Київ, 2021. В роботі вирішено актуальну науково-прикладну проблему щодо розробки моделей та методів забезпечення безпеки (доступності, конфіденційності) та якості обслуговування в комп'ютерних системах з урахуванням самоподібних властивостей інформаційних потоків в умовах наявності вторгнень та кібератак. Вперше розроблено концепцію забезпечення інформаційної безпеки комп'ютерних систем із самоподібними інформаційними потоками, які працюють в умовах вторгнень та кібератак; удосконалено модель розподіленої комп'ютерної системи, яка, на відміну від існуючих, включає компоненти забезпечення безпеки та управління вхідними інформаційними потоками з мультифрактальними властивостями; удосконалено метод забезпечення безпеки мережі при динамічному

балансуванні навантаження з самоподібним трафіком, який, на відміну від існуючих, відрізняється застосуванням моделі балансувальника комп'ютерної мережі з урахуванням параметрів безпеки розподілу трафіка і мультифрактальних властивостей трафіка; вперше розроблено метод динамічного балансування трафіка, який базується на моделі мережної системи виявлення вторгнень, що враховує мультифрактальні властивості трафіка та обмеження на час обслуговування різних класів трафіка; вперше розроблено метод забезпечення безпечної маршрутизації під час передачі самоподібного трафіка, який базується на мультифрактальних властивостях трафіка та параметрах якості обслуговування різнопріоритетного трафіка; вперше розроблено комплексний метод виявлення вторгнень, який базується на використанні алгоритму аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів з урахуванням ймовірності виявлення вторгнень; набули подальшого розвитку методи виявлення вторгнень на основі аналізу сигнатур, який враховує дані глибокого аналізу пакетів та рейтингування бази сигнатур; аналізу ентропії пакетів, який базується на розрахунку умовної ентропії та статистичних характеристиках даних пакетів; на основі машинного навчання, які базуються на мультифрактальних та рекурентних характеристиках трафіка. Реалізація результатів дослідження дозволяє забезпечити безпечну маршрутизацію за рахунок блокування у 8 раз більшої кількості атакованого трафіка, ніж під час роботи стандартного методу маршрутизації, зменшити джитер на 20%; забезпечити безпечне балансування самоподібних інформаційних потоків зі зниженням удвічі кількості втрачених даних, у 9 разів знизити кількість атакованого трафіка на серверах, на 16% знизити дисбаланс завантаження системи; забезпечити балансування навантаження в мережних системах виявлення вторгнень зі збільшенням кількості проаналізованих пакетів на 21%, за рахунок чого відсоток виявлених атак збільшився на 14% та зменшився середній час очікування пакетів на 16%; збільшити ймовірність виявлення вторгнень до 98%, зменшити відсоток невиявлених атак на 11%, отримати низьку кількість хибнопозитивних спрацьовувань (менше 8%) та зменшити кількість втрачених даних на 32% порівняно з аналогічними характеристиками існуючих систем забезпечення доступності, конфіденційності та якості обслуговування. Впроваджено – в навчальному процесі кафедри інфокомунікаційної інженерії ім. В.В. Поповського Харківського національного університету радіоелектроніки (ХНУРЕ): у лекційних курсах та практичних заняттях з дисциплін «Захист систем електронної комерції», «Системи інформаційної безпеки» під час підготовки студентів спеціальності 125 «Кібербезпека», в науково-дослідних роботах «Автоматизована оптична інформаційно-вимірювальна система для полігонних випробувань керованих та некерованих ракет, артилерійських і реактивних снарядів» (ДР №01190U001405), на підприємстві Харківського державного регіонального науково-технічного центру з питань технічного захисту інформації, ПрАт Фарлеп-Інвест, ТОВ Дайтекс Технолоджіс, АТ БАНКОМЗВ'ЯЗОК, ТОВ WorkNest, ТОВ Владармет. Галузь використання – кібербезпека в комп'ютерних системах

2. Dissertation for the Doctor of Technical Sciences degree in the specialty 05.13.21 «Information security systems». – Kharkiv National University of Radio Electronics. – State University of Telecommunications, Kyiv, 2021. An actual scientific and applied problem of developing models and methods of ensuring security (availability, confidentiality) and service quality in computer systems based on self-similar properties of information flows in the presence of intrusions and cyberattacks is solved in the thesis. The concept of ensuring information security of computer systems with self-similar information flows, which work in the conditions of intrusions and cyber attacks, was developed; the model of distributed computer system has been improved, which, in contrast to the existing ones, includes components of security ensuring and management of input information flows with multifractal properties; the method of ensuring network security in the course of dynamic load balancing with self-similar traffic has been improved, which, in contrast to the existing ones, differs in application of the computer network balancing model taking into account traffic distribution security parameters and multifractal traffic properties; the method of dynamic traffic balancing based on the network intrusion detection system model was developed and takes into account multifractal properties of traffic and service limitations for different traffic classes; the method of secure routing in case of transfer of self-similar traffic based on multifractal properties of traffic and quality of service parameters of priority traffic has been developed; the complex method of intrusion

detection has been developed, based on the use of signature analysis algorithm, analysis of network behavior anomalies and entropy analysis of protocols taking into account the probability of intrusion detection; intrusion detection methods based on signature analysis have been further developed, taking into account data from deep packet analysis and signature database ranking; packet entropy analysis based on conditional entropy calculation and statistical characteristics of these packets; machine-based training based on multifractal and recursive traffic characteristics. The implementation of the proposed concept, models and methods can provide secure routing by blocking 8 times more attacked traffic than the standard routing method, reduce jitter by 20%; to ensure secure balancing of self-similar information flows with a halving of the amount of lost data, to reduce the amount of attacked traffic on the servers by 9 times, to reduce system load imbalance by 16%; to provide load balancing in network intrusion detection systems with a 21% increase in the number of analyzed packets, thereby increasing the percentage of detected attacks by 14% and decreasing the average wait time for packets by 16%; to increase the probability of intrusion detection to 98%, to decrease the percentage of detected attacks by 11%, obtain a low false positive rate (less than 8%) and a 32% reduction in lost data compared to the same performance of existing availability, privacy and quality of service systems. . Implemented in the educational process of V.V. Popovskyy Department of Infocommunication Engineering of Kharkiv National University of Radioelectronics (KNURE): in lecture courses and practical classes on the disciplines «Security of electronic commerce systems», «Information security systems» in the training of students of the specialty 125 «Cybersecurity», in research works «Automated optical information and measurement system for polygon tests of guided and unguided missiles, artillery and missiles» (SR №01190U001405), at the Kharkiv State Regional Scientific and Technical Center for Technical Information Protection, PJSC Farlep Invest, LLC Dytex Technologies, JSC BANKOMSVYAZ, LLC WorkNest, LLC Vladarmet. The field of application is cybersecurity in computer systems.

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. Кіріченко Людмила Олегівна
2. Kirichenko Lyudmyla Olegivna

Кваліфікація: д. т. н., 01.05.02

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. Кіріченко Людмила Олегівна

2. Kirichenko Lyudmyla Olegivna

Кваліфікація: д. т. н., 01.05.02

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. Хорошко Володимир Олексійович

2. Khoroshko Volodymyr Oleksiiovych

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

Власне Прізвище Ім'я По-батькові:

1. Політанський Леонід Францович

2. Politanskyi Leonid Frantsovych

Кваліфікація: д.т.н., 05.27.01

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. Чевардін Владислав Євгенович

2. Chevardin Vladyslav

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Савченко Віталій Анатолійович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Савченко Віталій Анатолійович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.