Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U002803

Особливі позначки: відкрита

Дата реєстрації: 30-07-2024

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Сагайдак Віктор Анатолійович
2. Viktor Sahaidak

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 123

Назва наукової спеціальності: Комп'ютерна інженерія

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп'ютерна інженерія

Дата захисту: 12-08-2024

Спеціальність за освітою: Телекомунікації та радіотехніка

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.861.014

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

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

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.53.19, 50.37.23, 20.55.03, 20.56.01

Тема дисертації:

1. Методи підвищення ефективності виявлення шахрайства на мобільній мережі за допомогою комплексного використання CDR з різних джерел

2. Methods of improving the effectiveness of fraud detection on the mobile network by means of the integrated use of CDRs from various sources

Реферат:

1. Для досягнення мети дослідження, а саме підвищення ефективності процесу виявлення шахрайської діяльності за рахунок комбінації потоку деталізованих записів з комутаторів разом з стандартизованими форматами, наприкінці розділу були сформовані наступні наукові завдання: 1. Дослідити методи порівняння даних з мережного зонду для виявлення негативного впливу на роботу мережних елементів. 2. Проаналізувати методи моніторингу даних віртуалізованого середовища з резервуванням. 3. Дослідити потік CDR даних з IMS комутаторів та розробити алгоритм взаємодії системи розрахунку з системою моніторингу. 4. Визначити складові архітектури системи аналітики великих даних у залежності від джерела інформації та розробити схему етапів виявлення шахрайства. 5. Розрахувати показники оцінки середньозваженого

значення часу затримки для визначення ефективності розробленого інтерфейсу на тестовому середовищі, що імітує роботу інформаційної мережі. У другому розділі проводиться аналіз впливу шахрайства на інфокомунікаційну мережу, основні види, технології, що використовуються для реалізації того чи іншого виду шахрайства та основні ознаки шахрайської атаки або діяльності. Було проаналізовані складові NRTRDE та TAP3, передумови їх виникнення, типи сервісів для передачі та їх недоліки. Детальна увага була приділена безпосередньому збору даних з мережі за допомогою мережного зонду. Розглянуто такі технології як оптичні відгалужувачі та віддзеркалення трафіку з портів, наведено основні засади під час інтеграції з елементами мережі. Було досліджено аспекти інтеграції віртуалізованого середовища в інфокомунікаційну мережу та його експлуатацію, що здійснюють вплив на процес аналітики та виявлення шахрайства. У третьому розділі дисертації розглянуто теоретичні аспекти та практичне застосування розробленого алгоритму за допомогою комплексного використання деталізованих записів. Були наведені елементи тестової мережі vEPC та схема взаємодії джерел даних з системою виявлення шахрайства на базі RDBMS Oracle. Була наведена загальна схема обробки трафіку та створено коефіцієнти визначення ефективності на основі часових проміжків з використанням середньозваженого значення. Деталізовані записи IMS платформи дозволили створити доповнений CDR, що може бути завантажений у БД для подальшого аналізу системою виявлення шахрайства. Основна увага приділяється програмній реалізації цього алгоритму, який базується на інтеграції bash кодування разом з інструментарієм ODI для трансформації формату полів та розрахунку наданих сервісів з наступним завантаження у БД Oracle. Розділ надає детальний опис кожного процесу та демонструє продуктивність розробленого інтерфейсу на основі методу визначення ефективності, який базується на використанні часових проміжків середньозваженого значення. Були отримані наступні наукові результати: 1. Отримав подальшого розвитку метод моніторингу віртуалізованого середовища з резервуванням, який на відміну від існуючих дозволив виявити дублікацію даних, встановлення додаткового мережного зонду під час розширення мережі для удосконалення моделі підтримки її інфраструктури. 2. Розроблено алгоритм взаємодії IMS комутатора з системою виявлення шахрайства та розрахунку послуг, наукова новизна якого полягає у використанні доступного bash кодування для форматування деталізованих записів, що базуються на застосуванні інструментів інтеграції даних, який дозволяє створити інтерфейс з наступним завантаженням інформації безпосередньо у базу даних системи моніторингу. 3. Вперше розроблено метод оцінки ефективності системи розпізнання шахрайства, що ґрунтується на статичному методі з використанням вагомого коефіцієнту, на основі комплексного використання деталізованих записів, який дозволив зменшити середньовагоме значення часу затримки даних у 3.7 разів для NRTRDE та у 14 разів для TAP3. Дисертація виконувалась в Державному університеті інформаційно-комунікаційних технологій. Обраний напрям досліджень відповідає тематиці науково-дослідних робіт Державного університету інформаційно-комунікаційних технологій. Ключові слова: Моніторинг, безпроводова мережа, інформаційна затримка, аналіз даних, статистичні моделі, текстова інформація, модель, система реального часу, машинне навчання, база даних, система виявлення вторгнень, контроль трафіку, інформаційна безпека, хмарні обчислення, статистичний аналіз.

2. To achieve the goal of the research, namely to increase the effectiveness of the process of detecting fraudulent activity due to the combination of the flow of detailed records from switches together with standardized formats, the following scientific tasks were formed at the end of the chapter: 1. Investigate methods of comparing data from a network probe to identify a negative impact on the operation of network elements. 2. Analyze data monitoring methods of a virtualized environment with redundancy. 3. Investigate the flow of CDR data from IMS switches and develop an algorithm for the interaction of the calculation system with the monitoring system. 4. Determine the components of the architecture of the big data analytics system depending on the source of information and develop a scheme of fraud detection stages. 5. Calculate the evaluation indicators of the weighted average value of the delay time to determine the effectiveness of the developed interface on a test environment that simulates the operation of an information network. The second section analyzes the impact of fraud on the information and communication network, the main types, technologies used to implement one or another type of fraud, and the main signs of a fraudulent attack or activity. The components of NRTRDE and TAP3, the prerequisites for their

occurrence, the types of services for transmission and their shortcomings were analyzed. Detailed attention was paid to the direct collection of data from the network using a network probe. Such technologies as optical splitters and mirroring of traffic from ports are considered, the basic principles during integration with network elements are given. Aspects of the integration of the virtualized environment into the information communication network and its operation, which influence the process of analytics and fraud detection, were investigated. In the third chapter of the dissertation, the theoretical aspects and practical application of the developed algorithm are considered with the help of complex use of detailed records. The elements of the vEPC test network and the scheme of interaction of data sources with the fraud detection system based on RDBMS Oracle were given. A general scheme of traffic processing was given and performance coefficients were created based on time intervals using a weighted average value. The detailed records of the IMS platform made it possible to create a supplemented CDR, which can be loaded into the database for further analysis by the fraud detection system. The main attention is paid to the software implementation of this algorithm, which is based on the integration of bash coding together with the ODI toolkit for the transformation of the field format and the calculation of the provided services, followed by uploading to the Oracle database. The section provides a detailed description of each process and demonstrates the performance of the developed interface based on the time-weighted average performance method. The following scientific results were obtained: 1. The method of monitoring a virtualized environment with redundancy received further development, which, unlike the existing ones, made it possible to detect data duplication, install an additional network probe during network expansion to improve the model of supporting its infrastructure. 2. An algorithm for the interaction of the IMS switch with the fraud detection and service calculation system has been developed, the scientific novelty of which is the use of available bash coding for formatting detailed records based on the application of data integration tools, which allows creating an interface with subsequent uploading of information directly into the monitoring system database. 3. For the first time, a method for evaluating the effectiveness of a fraud detection system based on a static weighting method was developed, based on the comprehensive use of detailed records, which allowed to reduce the weighted average data delay time by 3.7 times for NRTRDE and 14 times for TAP3. The dissertation was completed at the State University of Information and Communication Technologies. The chosen direction of research corresponds to the topic of research works of the State University of Information and Communication Technologies. Key words: Monitoring, wireless network, information latency, data analysis, statistical models, text information, model, real-time system, machine learning, database, intrusion detection system, traffic control, information security, cloud computing, statistical analysis.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Алтинніков Д. Є., Шевченко О. О., Бердник І. І., Зуб О. В., Сагайдак В. А., «Використання Java-анотацій як інструменту надання API», Зв'язок, № 4(152), с. 56–59, 2021.
- Сагайдак В. А., Сеньков О. В., «Huawei Genex Discovery – інструмент виявлення великих даних для аналізу безпроводової мережі», Зв'язок, № 4(158), с. 34–41, 2022.
- Сагайдак В. А., Лисенко М. М., Сеньков О. В., «Шахрайство у сфері телекомунікацій та його вплив на бізнес операторів зв'язку», Зв'язок, № 6(160), с. 17–20, 2022.
- Сагайдак В. А., «Огляд систем розпізнання шахрайства та розробка коефіцієнтів для визначення їх ефективності», Кібербезпека: освіта, наука, техніка, № 3 (23), с. 274-283, 2024.

- Сачук О. В., Сагайдак В. А., «Розроблення методики транскрибації на основі нейронних мереж», Зв’язок, № 2(168), с. 23-26, 2024.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Сторчак Каміла Павлівна

2. Kamila P. Storchak

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0001-9295-4685

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Жураковський Богдан Юрійович

2. Bogdan Zhurakovskyi

Кваліфікація: д.т.н., професор, 05.12.02

Ідентифікатор ORCID ID: 0000-0003-3990-5205

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Голубничий Олексій Георгійович
2. Oleksii Holubnychyi

Кваліфікація: д. т. н., доц., 05.12.02

Ідентифікатор ORCID ID: 0000-0001-5101-3862

Додаткова інформація:

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Вишнівський Віктор Вікторович
2. VIKTOR VYSHNIVSKYI

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0003-1923-4344

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Лемешко Андрій Вікторович
2. Andrii V. Lemeshko

Кваліфікація: д.філософ, доц., 123

Ідентифікатор ORCID ID: 0000-0001-8003-3168

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Бондарчук Андрій Петрович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Бондарчук Андрій Петрович
Відповідальний за підготовку облікових документів	Лазоренко Л.М.
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна