# Облікова картка дисертації

## I. Загальні відомості

**Державний обліковий номер:** 0419U000145

**Особливі позначки:** відкрита

**Дата реєстрації:** 11-01-2019

**Статус:** Захищена

**Реквізити наказу МОН / наказу закладу:**

## II. Відомості про здобувача

**Власне Прізвище Ім'я По-батькові:**

1. Дєєв Костянтин Сергійович
2. Deev Kostiantyn Serhiiovych

**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:** 26-12-2018

**Спеціальність за освітою:** Радіофізика і електроніка

**Місце роботи здобувача:** Черкаський національний університет імені Богдана Хмельницького

**Код за ЄДРПОУ:** 02125622

**Місцезнаходження:** бульв. Шевченка, 81, м. Черкаси, Черкаський р-н., Черкаська обл., 18031, 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):** К 73.052.04

**Повне найменування юридичної особи:** Черкаський державний технологічний університет

**Код за ЄДРПОУ:** 05390336

**Місцезнаходження:** бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, 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:** Київський національний університет імені Тараса Шевченка

**Код за ЄДРПОУ:** 02070944

**Місцезнаходження:** вул. Володимирська, 60, м. Київ, Київська обл., 01033, Україна

**Форма власності:**

**Сфера управління:** Міністерство освіти і науки України

**Ідентифікатор ROR:** Не застосовується

## V. Відомості про дисертацію

**Мова дисертації:**

**Коди тематичних рубрик:** 20.51, 28.15

**Тема дисертації:**

1. Дослідження мережевої взаємодії за допомогою системи глибокого аналізу пакетів
2. The study of networking interactions by using deep packet inspection system

**Реферат/анотація:**

1. У дисертації запропоновано методи забезпечення ідентифікації мережевої активності однорангових додатків для наступної їх класифікації та виділення в окремий сервісний клас такої взаємодії з метою проведення гнучкої тарифікації у мережі оператора Інтернет-послуг. Реалізація створених моделей і методів у програмних засобах та їх впровадження у тестових сегментах розподілених мереж операторів послуг дало можливість значною мірою підвищити ефективність надання послуг користувачам та використовувати оптимальні політики управління мережевим трафіком. У роботі окреслено підходи до стандартизації та реалізації у програмних платформах функцій аналізу пакетного навантаження згідно з їх представленням у вигляді багаторівневої моделі взаємодії відкритих систем OSI. Визначено функціональний рівень та надано рекомендації щодо оптимального розміщення комплексу аналізатора в операторській мережі загального призначення. Розглянуто можливості часткової віртуалізації окремих компонентів системи з метою підвищення загальної пропускної здатності. Ключові слова: глибока інспекція мережевих пакетів, аналіз

трафіку, класифікація пакетів, система запобігання вторгненням, засоби моніторингу мережі.

2. The Thesis introduces models of representing Peer-to-Peer networking interactions and proper methods of conducting IP packet header and payload analysis. This area has been already heavily investigated by many scientists, however there are few questions still open. As Internet is growing and becoming more popular, the number of concurrent data flows starts to increase, which makes sense in amount of bandwidth requested and that should be analyzed respectively. In this work, the methods for ensuring identification of network activity of Peer-to-Peer applications for their subsequent classification and proper allocation to separated service class are offered. Such interaction by being classified provides ability to implement flexible charge policy in service-provider network. That should considerably increase user's experience and lower overall capacity load on backbone infrastructure links. Service-providers and corporate customers need the ability to identify Peer-to-Peer interactions, because they are generally not directly related to workflow and lead to premature exhaustion of the available bandwidth of external links. This Thesis represents the principles of building system, which searches for Peer-to-Peer interaction in live network traffic and then places such conversation into formerly marked QoS class with bandwidth constraints. The implementation of the created models and used methods in software has significantly increased the efficiency of provided services. To ensure high quality service to all its subscribers it is desirable to create the system that carries identification of such flows based on classes of service with different priorities. It was tested in specific segments of service-provider's distributed networks and have shown that optimal policies for managing network traffic considerably simplifies management of complex setup. With consistently increasing number of packets per second that should be investigated, the analysis using standard server's hardware-based solutions is challenging, as it is necessary to distribute the load over multiple systems. Therefore, the best way is to use special software-defined complex rather than hardware implementations. Software will distribute the load in the internals of the complex, using the principles and approaches, in particular, described in this paper. Throughput of the system configured in the same manner was analyzed though. The paper outlines the approach with standardization and implementation packet payload analysis functions in software platforms according to their representation in the form of a multilevel OSI model. The functional level is determined and recommendations for the optimal placement of the analyzer complex in service provider network are given. Outlined methods and approaches in the implementation of flexible network packet classifying system are based on deep packet inspection technique. Highlighted approach is analyzed, its benefits are determined to approximate the value of suggested improvements in terms of throughput. Regular expressions matching can balance classified packet payload and could be used for parallel execution on multiple specialized nodes. The possibilities of partial virtualization of individual components of the system with the purpose of increasing the overall throughput are also considered and recommendations are provided. The Thesis presents a flexible approach to match network packet via search engine using relaxed regular expressions for whole network layer headers. By using such mechanism, software and hardware composition that might be used as a detector of anomalies in the network has been created finally. Further improvements to the scope of network classification will be performed based on created method of applications interaction identification which rooted on supervised automated machine learning techniques coupled with specific composed training data publicly available for consideration. The results of Thesis are helpful in terms of practical experience, which can be applied to development of scalable packet classifying system with limited budget on set of available hardware. Keywords: deep packet inspection, traffic analysis, packet classifying methods, intrusion detection system, network monitoring tools.

### 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. Бойко Юрій Володимирович
2. Boiko Yurii Volodymyrovych

**Кваліфікація:** к. ф.-м. н., 01.04.10

**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. Мусієнко Максим Павлович
2. Musienko Maksim

**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. Бараннік Володимир Вікторович

2. Barannik Volodymyr Viktorovych

**Кваліфікація:** д. т. н., 05.12.02

**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** Рудницький Володимир Миколайович

**Власне Прізвище Ім'я По-батькові головуючого на засіданні** Рудницький Володимир Миколайович

**Відповідальний за підготовку облікових документів**

**Реєстратор**

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