СТАНОВИЩЕ

от проф. д.м.н. **Евгений Христов НИКОЛОВ**

член на жури по чл. 4 от Закона за развитие на академичния състав в Република България

(обн. ДВ38/21.05.2010, изм. ДВ81/15.10.2010, изм. ДВ101/28.12.2010)

съгласно решение на Факултетния съвет на Факултет по математика и информатика,

на Софийски университет „Климент Охридски“, от 02.07.2012, протокол № 6)

във връзка със защитата на гл. ас. **Стела Иванова РУСЕВА**

докторант на самостоятелна подготовка

по професионално направление 4.6 Информатика и компютърни науки

(01.01.12 Информатика – Компютърни мрежи и архитектури)

на тема „*Изграждане на система за защита от DDoS атаки*“

за присъждане на образователната и научна степен „доктор“

с научен ръководител проф. д-р **Нина Василевна СИНЯГИНА**

Представената дисертация съдържа 154 страници, структурирани, както следва: съдържание, речник на термините, въведение, глава 1 „*Атаки от типа DoS и DDoS*“, глава 2 „*Методи и средства за защита на HTTP сървър*“, глава 3 „Изграждане на математически модел, описващ взаимодействието на сървъра с клиентите“, глава 4 „Ruslan – система за защита от DDoS атаки“, Заключение,Научно-приложни приноси на дисертацията, Приложение 1 – Скрипт за iptable, Приложение 2 – Публикации, свързани с дисертационния труд, Приложение 3 – Използвана литература.

Във **въведението**, ясно и точно са посочени причините, които определят избраната тема като значима и полезна, след което е формулирана реална и постижима цел на дисертационния труд: „*Изследване на методи и начини за защита на компютърна система от DDoS атаки, които позволяват получаване на оптимална сигурност и достъпност на ресурсите*“. На тази основа са поставени, балансирано и прецизно, конкретните задачи „*(1) Определяне на оптимална конфигурация на системата за защита от DDoS атаки; (2) Създаване на модел на система за защита, описващ взаимодействието на сървъра и клиентите; (3) Разработка на алгоритми и програмна реализация на системата за защита; (4) Имплементация на комплекс от програмни средства, предпазващи от DDoS атаки и експериментална верификация на създадените средства.*“

В **първа глава** е направен сполучлив обзор на различните видове атаки „отказ от обслужване“ с описание на начина на функционирането им, както и на метода на тяхното откриване и блокиране. Представено е коректно състоянието на проблема и е предложена много добра класификация на този род атаки. Показани са по един добър начин най-перспективните разработки в областта „защита на компютърните мрежи“, свързана със защитата от DDoS атаки.

Във **втора глава** е представен, обективно и точно, разширен анализ на начините за изграждане на система за защита. Избрана е x86 архитектура, ОС GNU/Linux (CentOS 6), HTTP сървър Apache 2.2, PHP 5.3, MySQL5.0, мрежов филтър netfiter.

В **трета глава** е представен един коректен модел на системата, описващ взаимодействието на сървъра с клиентите, отчитащ характеристиките на компютърната мрежа и на защитавания сървър. Представен е също и коректен модел, отчитащ загубата на пакети в мрежата, причинена от TCP SYS атака.

В **четвърта глава** е направено едно сполучливо описание на програмната реализация на система за защита, получила името Ruslan (събирателно от трите имена на автора: **Rus**eva Ste**la** Iva**n**ova). Определени са компонентите, алгоритмите, конфигурацията на елементите и настройката на параметрите, позволяващи оптимална защита на уеб сървър от DDoS атаки. Представена е експериментална проверка и анализ на получените резултати.

На основа на запознаване с материалите от дисертацията, като член на Научното жури, мога да потвърдя научно-приложните приноси на дисертанта, формулирани по следния начин: *„(1) Извършена е класификация и анализ на известните видове DDoS атаки и методите за борба с тях; (2) Дефинирани са базовите променливи за конфигуриране на защитните механизми за LAMP сървър за противодействие на DDoS атаките, като са определени средствата за противодействие на DDoS атаките и нивата на защита за уеб сървър. Изследвани са методите за изграждане на противодействаща система срещу DDoS атаките; (3) Създаден е модел на системата, описващ взаимодействието на сървъра с клиентите, отчитащ характеристиките на компютърната мрежа и защитавания сървър. С помощта на математическия апарат на теорията на системите за масово обслужване са определени допустимите интервали за броя на полуотворените TCP съединения на сървъра. Описаният математически модел позволява откриването на атаката и е устойчив към рязкото нарастване на интензивността на входящия поток от заявки за сървъра, при което се отчитат характеристиките на мрежата и на защитавания сървър; (4) Разработена е система за защита Ruslan, целяща блокиране на DDoS атаките. Системата променя параметри на ядрото на ОС, основни конфигурационни файлове и съдържа допълни модули; (5) Експериментално е доказана стабилната работа на системата Ruslan при реално проведени DDoS атаки. Потвърдена е способността й за запазване на работоспособността на уеб сървъра.*“

В заключение, като член на Научното жури, изразявам СЪГЛАСИЕ с твърдението, че представената от гл. ас. Стела Иванова РУСЕВА дисертация за присъждане на образователната и научна степен „доктор“, отговаря НАПЪЛНО на изискванията на Закона за развитие на академичния състав в Република България и приканва останалите членове на научното жури да изразят подобно съгласие.

30.08.2012 г., София

Проф. д.м.н. Евгений Христов Николов