Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Andrej Nad'** **Oponent:** **David Janota**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2017/2018**

Téma diplomové práce: **Implementácia Diehard testov pre testovanie generátorov pseudonáhodných čísel**

Hodnocení práce:
Práce diplomanta se zabývá implementací validačních testů s názvem DieHard, jejichž cílem je prověřit dostatečnou kvalitu generátoru náhodných (resp. pseudonáhodných) čísel ve smyslu dostatečné míry náhodnosti. Práce je rozdělena do celkem 9 kapitol včetně úvodu a závěru, kromě teoretické a praktické části jsou přiloženy také zdrojové kódy v jazyce Python.

Aktuálnost zvoleného tématu hodnotím jako vysokou, kybernetická bezpečnost a s ní související šifrování, které je na náhodných čísel založeno je v současné době bez diskuse jedno z top témat celého světa. Obtížnost úkolu zejména po stránce praktické hodnotím jako spíše náročnější, diplomant musel provést analýzu a tvorbu kódu pro velké množství testů, kromě toho je všechny otestovat na různých generátorech a srovnat výsledky. V závěru je proveden test několika generátorů, např. v MS Excel 2013 nebo knihovnách jazyka C.

Při čtení jsem byl velmi příjemně překvapen, jak kvalitně a technicky na úrovni se diplomant celého úkolu zhostil. Práce se velmi dobře čte, tvoří ucelenou technickou zprávu, není vynecháno žádné téma, testy jsou přehledně srovnány a vyhodnoceny. U každého testu je popsán algoritmus a jeho vyhodnocení, což může bez znalosti zbytku práce výborně posloužit jako návod na vlastní implementaci testů. Na vysoké úrovni je také samotný zdrojový kód.

Prakticky jediné drobné negativum jsou občasné překlepy(TESOTVANIE) a drobné gramatické chyby. Doporučil bych také provést test na generátoru, o kterém víme, že neprojde testy (již zmiňovaný MS Excel 2003) s cílem provést negativní testování.

Konstatuji, že diplomant podle mého názoru zcela splnil podmínky zadání, doporučuji jednoznačně k obhajobě.

Dotazy:
1. Má výsledná podmínka pro hodnotu testu P(někde také p)<=0,01 nějaký význam v oblasti testování hypotéz?
2. Větu "Drobné rozdiely sú spôsobené tým, že môj program vracia presnejšie výsledky, ako sú očakávané" bych poprosil rozvést, proč tomu tak je.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 1. 6. 2018 Podpis oponenta diplomové práce