prof. Ing. Jan Čapek, CSc.,
Ústav systémového inženýrství a informatiky,
Fakulta ekonomicko-správní, Univerzita Pardubice.

Posudek disertační práce.

Autor:	Mgr. Tomáš Žižka
Školitel:	doc. Ing. Jan Skrbek, Dr.
Studijní program:	P6209 - Systémové inženýrství a informatika
Studijní obor:	6209V003 – Ekonomická informatika

Název práce: Cílená distribuce informací

Předložená disertační práce (DP) má 111 stran textu s obrázky, tabulkami a 4 strany příloh. DP je rozdělena do osmi kapitol a závěru práce. V první kapitole jsou uvedeny cíle práce a přínosy, druhá kapitola je věnována analýze současného stavu a je dále rozdělena do dvou podkapitol. Třetí kapitola se zabývá požadavky na efektivní systém včasného varování. Čtvrtá kapitola se věnuje popisu modelových situací, pátá kapitola je zasvěcena pozičnímu šifrování a šestá kapitola se zabývá algoritmem AES. Sedmá kapitola naplňuje cíl práce a zabývá se návrhem konceptuálního řešení, v osmé kapitole je rozebráno ekonomicko-implementační hledisko. Závěr obsahuje shrnutí DP.
Dále se vyjádřím k:

- Aktuálnosti zvoleného tématu dizertační práce.
- Splnění sledovaného cíle.
- Zvoleným metodám zpracování dizertační práce.
- Dosaženým výsledkům dizertační práce a přínosy pro další rozvoj vědy a techniky
- Publikační činnosti doktoranda

Aktuálnost zvoleného tématu dizertační práce.

Není pochyb o tom, že zaměření na systém včasného varování před vzniklými krizovými situacemi je velice aktuální. S pokroky v informačních a komunikačních technologiích a neutuchajícími různými druhy katastrof, mimořádných událostí a nehod nabývají systémy včasného varování na důležitosti.

Splnění sledovaného cíle.

Po prostudování DP mohu prohlásit, že dizertantem vytčené cíle, které jsou podrobně popsány v první kapitole, jsou splněny.

Zvolené metody zpracování dizertační práce.

Dizertant při zpracování DP použil základní vědecké metody, nejprve analýzou současného stavu řešené problematiky (podrobně rozvedenou ve druhé kapitole) zjistil slabá místa, například, že v krizové komunikaci chybí aspekt doručení aktuálně potřebné informace k zamýšlenému příjemci. Z toho potom vyplynula řešení problému.

Dosažené výsledky dizertační práce a přínosy pro další rozvoj vědy a techniky
Za přínos práce lze považovat zejména rešerši problematiky aktuálního stavu včasného varování a navrženou metodiku přenosu varovných šifrovaných zpráv cíleným příjemcům.

Publikační činnost doktoranda
Dizertant uvádí celkem 20 titulů publikační činnosti, z nichž pouze dva výsledky jsou v časopisech indexovaných v databázi SCOPUS. Zbylých 18 výsledků je publikováno ve sbornících různých typů konferencí.

Připomínky a otázky k dizertační páci:
Str. 44 obr. 9. uvádíte „vlastní zpracování" ale je to modifikace obr. 13 v disertační práci ing. Kubáta.
Str. 59 V DP uvádíte „*Šifrovací funkce musí být vytvořena tak, aby kryptogram odolal útočníkovi po určitou dobu, která se označuje jako* ***doba rezistence kryptogramu****.*"
Jak dlouhé doby máte na mysli vzhledem k včasnému varování?

Str. 65 V DP uvádíte „*Podle výpočtů získaných na základě tzv. Groverova prohledávacího algoritmu (Grover's algorithm) by prolomení 128 bitové varianty AES (AES-128) v případě použití kvantové technologie trvalo pouhých šest měsíců*"
Z tohoto pohledu je navrhované použití AES šifry neodůvodněné a zbytečně komplikované,

Str. 83 a další s hexadecimálním vyjádřením znaků nemůžete provádět operaci XOR.

Str. 84 poslední řádek by měl být označen jako w[7] a ne w[6].

V jakém vztahu je Vaše DP k DP ing. Kubáta?

Jsem přesvědčen, že pro potřeby včasného varování by posloužil systém blokového šifrovače v uspořádání ECB (Electronic Code Book).

Závěr:
Není pochyb o tom, že návrh konceptuálního řešení systému, který bude schopen distribuovat varovné informace do určité předem vymezené oblasti je velice aktuální. Dizertační práce je přínosná pro další rozvoj oboru. **Doporučuji disertační práci k obhajobě** před příslušnou komisí a

n a v r h u j i

aby po úspěšné obhajobě byl Mgr. Tomáši Žižkovi udělen akademický titul Philosophiae Doctor ve zkratce Ph.D.

V Pardubicích dne 18. 4. 2018

Oponentní posudek disertační práce

Název práce: Cílená distribuce informací.

Autor: Ing. Tomáš Žižka
Školitel: doc. Ing. Jan Skrbek, Dr., Ekonomická fakulta, Technická Univerzita Liberec
Oponent: prof. RNDr. PhDr. Antonín Slabý, CSc., Fakulta informatiky a managementu, Univerzita Hradec Králové

Struktura a obsah práce

Práce je věnována problematice cílené distribuce informací v průběhu mimořádných a krizových situací.. Téma je užitečné a potřebné a lze dokonce konstatovat, že jeho aktuálnost vzrůstá. Práce řeší problematiku dosti komplexně a snaží se integrovat metody, přístupy a charakteristiky do jednotného metodologického postupu. Velká pozornost věnována vytvoření konceptuálního řešení .

Práce má 115 stran. Základní text práce je členěn na 8 číslovaných kapitol, úvod a závěr, a je doplněn o seznamy zkratek, obrázků, tabulek, použité literatury, autorovy publikační činnosti a přílohu.
Kapitola 1 obsahuje úvod do tématu práce, výzkumné otázky a cíle práce a velmi stručně se věnuje použitým metodám a struktuře práce. Kapitola 2 vymezuje pojmový aparát oblasti a způsoby současného řešení varovných systémů. Kapitola 3 je věnována požadavkům na efektivní systém včasného varování a kritickému zhodnocení stávajících systémů Kapitola 4 modeluje 4 různé fiktivní situace ohrožení, jejich specifika a řešení. Kapitola 5 se zabývá pozičním šifrováním a zaměřuje se na základy kryptografie, kryptografické systémy a jejich využití a úzce navazující kapitola 6 s zabývá využitím algoritmu AES v oblasti systémů varování. Důležitá kapitola 7 - Návrh konceptuálního řešení představuje autorovo řešení a jeho podrobnosti. Velká pozornost je věnována postupu vymezení oblasti a její formalizaci - Use case diagramům představujících rozhraní systému a způsoby interakcí jednotlivých aktérů se systémem včasného varování a diagramu aktivit představujícího procesní logiku systému. Stručná kapitola 8 se zabývá vybranými ekonomicko implementačními problémy. Následuje stručný závěr rekapitulující text a zdůrazňující vlastní autorovy přínosy.

Cíl práce, výzkumné otázky, aktuálnost tématu, soulad s oborem studia

Cílem práce je navržení konceptuálního řešení systému, který distribuuje varovné informace do zadané oblasti s atributem exklusivity.
K dosažení tohoto cíle stanovuje autor 5 postupných kroků: analýza současného stavu v oblasti systémů časného varování, stanovení požadavků na efektivní systém včasného varování včetně komponenty zajišťující šifrování, návrh modelových situací vycházejících z aktuálních hrozeb, analýza možných distribučních kanálů, konceptuální návrh řešení pro včasnou distribuci pozičně šifrovaných varovných informací (analýza a porovnání algoritmů a návrh vhodného algoritmu pro příjem varovné zprávy.

Autor formuluje následujících 5 výzkumných otázek:
Je možno nalézt řešení, které by eliminovalo či snižovalo míru nedostatků stávajících procesních přístupů a systémů ?
Lze zajistit, aby co největší počet potenciálně ohrožených občanů získal relevantní informace o míře nebezpečí ?
Lze navrhnout konceptuální model systému při vysoké funkčnosti a rozumných nákladech ?

Zohlednění optimální funkčnosti při co nejnižších nákladech.
Zajištění exkluzivity informace vzhledem k definované oblasti.
Postupná a cíleně řízená evakuace
Dílčí kroky jsou správně voleny a vedou k dosažení cíle. Téma a cíl práce jsou zajímavé a užitečné, náročné a velmi aktuální. Práce svojí tématikou patří do oboru Ekonomická informatika doktorského studijního programu Systémové inženýrství a informatika.

Použité vědecké metody v disertační práci
Práce vychází z rešerže a analýzy velmi rozsáhlých, ale různě kvalitních, někdy velmi obtížně dostupných literárních zdrojů o předmětné problematice. Zásadní pozornost je věnována způsobům získání relevantních dat a informací z různých zdrojů a jejich kritické zhodnocení. Ke zpracování datových zdrojů použil autor klasické a osvědčené metody a přístupy- deskripce, klasifikace, kritické zhodnocení. Dále jsou použity i metody abstraktního modelování k vytvoření modelových situací a metody analýzy a syntézy systémů při tvorbě konceptuálního návrhu, mezi tím vybrané diagramy UML k popisu systému včasného varování. Potenciál, který mají metody a jejich skupiny pro řešení problematiky je v práci podrobně a správně rozebrán. Metody je možno v souhrnu považovat za adekvátní, správné, z velké části klasické, osvědčení a ke splnění konkrétních cílů vedoucí.

Splnění cílů práce
Problematika řešená v práci je náročná, nejsou s ní dostatečné zkušenosti, je obtížně modelovatelná, dynamická.

Cíle práce byly splněny. K hlavnímu cíli práce a podobně ke všem dílčím krokům vedoucím k jeho dosažení přispěl autor věrohodným příspěvkem. Postupy a metody jsou aplikovány správně, a metodický rámec je dobře použitelný a dávající různé impulzy ke zlepšení stavu v oblasti distribuce varovných informací.

Přesnost práce, formální stránka práce
Práce je napsána stručným, jasným a přesným jazykem. Formální stránka práce i přesnost vyjadřování, úprava vzorců, diagramů obrázků a výstupů jsou na dobré úrovni. Práce má jasnou strukturu, proto je možno se v ní dobře orientovat.

Výsledky práce a poznatky a přínosy práce
Práce přináší výsledky v oblasti teoretické, metodologické i praktické.
Za hlavní teoreticko-metodologické výsledky lze považovat konceptuální řešení varovného systému s akcentováním jeho schopnosti distribuovat varovné informace do vymezené oblasti s atributem exklusivity s použitím pozičního šifrování v případě mimořádných událostí a popis podstatných funkčnostních a implementačních detailů tohoto systému.
Práce má i rozsáhlé potenciální využití praktické. Nabízí se využití postupů uvedených v práci. Za přínos lze považovat i pěkné a srozumitelné a dosti komplexní a v některých směrech hluboké zpracování tématiky s použitím adekvátních metod.

Publikační činnost autora ve vztahu k práci
Publikační činnost autora je z hlediska kvantitativního silně nadstandardní, neboť zahrnuje celkem 19 položek ve zdrojích adekvátních tématu práce. Publikační činnost potvrzuje nejen autorovu pracovitost a systematičnost, ale i dlouhodobý zájem o oblast, která je tématem disertační práce. Pozitivním rysem je navázání tématiky práce i publikačních aktivit na výzkum školitele a pracoviště.

Otázky do diskuse obhajobě

Práce ukázala zároveň, že problematika je náročná, nejsou s ní dostatečné zkušenosti, je obtížně modelovatelná. V důsledku toho musí být některé závěry poněkud obecné. Těchto skutečností si je autor dobře vědom.

Diskuse by se mohla týkat například následujících problémů:

Vývoj krizových situací patřících do jisté třídy má jistě některé společné rysy a znaky. Ale současně je vždy jedinečný, často překvapivý v některých aspektech. Je výběr 4 typových situací dostatečný z hlediska pokrytí oblasti a možných scénářů vývoje?

Je možné zahrnout i učení se na základě proběhlých krizových situací?

Jaký systém vzdělání a proškolení na straně obyvatelstva je nutný?

Je možné uvažovat o jiných formách využití kryptografie, které by vedly k efektivnějším způsobům vytvoření pozičně šifrované informace?

Závěr:

Práce splňuje v nároky na disertační práce kladené. Je nutno též konstatovat, že jde o zralou osobnost s delšími výzkumnými a publikačními aktivitami v oboru tématiky práce. Doporučuji, aby Ing. Tomáši Žižkovi byl po úspěšné obhajobě udělen titul Ph.D.

Hradec Králové 15.4.2018

Antonín Slabý