KOMPARÁCIA VÝSTUPNÝCH PARAMETROV PRI HODNOTENÍ ÚČINNOSTI BEZPEČNOSTNÝCH SYSTÉMOV

Juraj Vaculík[1], Tomáš Loveček[2]

ABSTRAKT

Článok popisuje rôzne kvantitatívne parametre, ktoré možno využiť pri hodnotení účinnosti bezpečnostných systémov. Porovnáva výhody a nevýhody dvoch základných výstupných parametrov - koeficientu účinnosti ochranných opatrení a pravdepodobnosti prerušenia za účelom stanovenia najlepšieho prístupu pri hodnotení účinnosti bezpečnostných systémov.

Kľúčové slová: koeficient účinnosti ochranných opatrení, pravdepodobnosť prerušenia

ABSTRACT

Article describes various qualitative output parameters for evaluation of efficiency of PPS. The main purpose is to compare two basic output parameters - index of security measures and probability of interruption and to define best approach in evaluation of efficiency.

Key words: index of security measures, probability of interruption

1 ÚVOD

Hodnotenie účinnosti bezpečnostných systémov možno chápať ako dôležitú úlohu v komplexnom procese hodnotenia kvality bezpečnostných systémov. Pre účel hodnotenia účinnosti bolo v minulosti zadefinovaných viacero výstupných parametrov, pomocou ktorých je možné určiť účinnosť. V článku skúmame otázku, ktoré z týchto parametrov najlepšie vystihujú reálnu účinnosť bezpečnostného systému a akým spôsobom treba pristúpiť k ich praktického výpočtu.

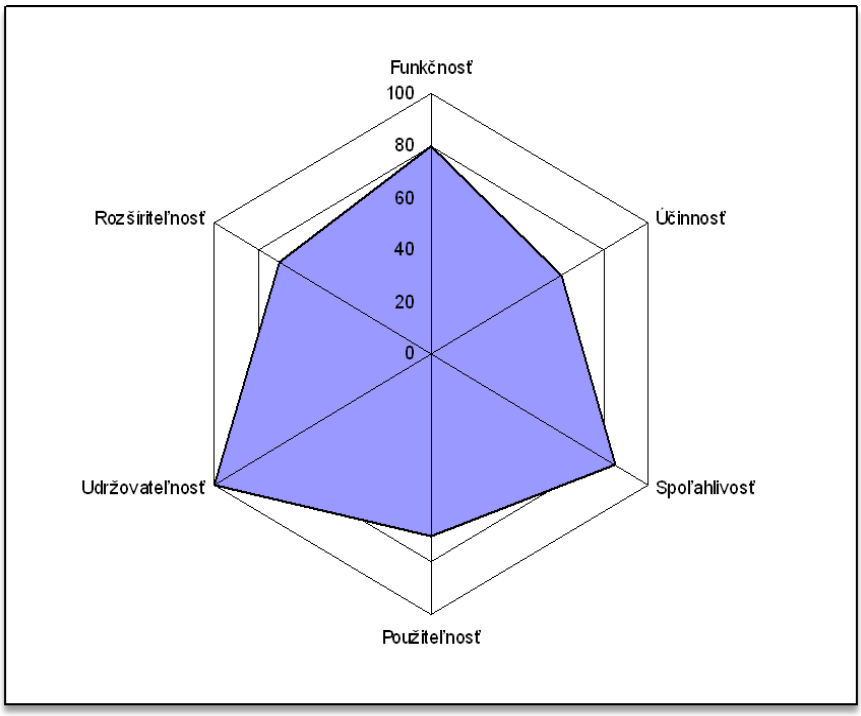
[1] Ing. Juraj Vaculík, Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, Ul. 1.mája 32, 01026 Žilina, Tel.: +421415136669, email: juraj.vaculik@fsi.uniza.sk
[2] doc. Ing. Tomáš Loveček, PhD., Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, Ul. 1.mája 32, 01026 Žilina, Tel.: +421415136664, email: tomas.lovecek@fsi.uniza.sk

1 KVALITA BEZPEČNOSTNÝCH SYSTÉMOV

Kvalita bezpečnostného systému predstavuje celkový súhrn znakov bezpečnostného systému, ktoré ho robia schopným uspokojovať určené a predpokladané potreby, teda zaistiť bezpečnosť v danom prostredí, čase a na stanovený účel.[7] Medzi skúmané znaky patrí :

- Funkčnosť – bezpečnostný systém má implementované všetky požadované funkcie,
- Účinnosť – bezpečnostný systém je schopný plniť funkcie rýchlo a efektívne,
- Spoľahlivosť – prvky plniace jednotlivé funkcie sú bezporuchové/redundantné,
- Použiteľnosť – všetky funkcie bezpečnostného systému sú optimalizované pre praktické použitie,
- Udržovateľnosť – všetky prvky plniace jednotlivé funkcie sú priebežne kontrolované a udržiavané v požadovanom technickom stave,
- Rozšíriteľnosť – možno jednoducho pridávať nové prvky a funkcie bezpečnostného systému podľa potreby.

Kvalitu bezpečnostného systému možno potom graficky znázorniť ako plochu nepravidelného šesťuholníka, ako ukazuje obr.1.



Obrázok 1 Grafické znázornenie kvality bezpečnostných systémov

Hodnotenie účinnosti bezpečnostných systémov úzko súvisí nielen s hodnotením kvality bezpečnostného systému, ale aj s procesom posudzovania rizík objektov. Posúdenie rizík je podľa [12] definované ako :

- Identifikácia rizík – proces hľadania, rozpoznávania a popisovania rizík,
- Analýza rizík – proces pochopenia povahy rizika a stanovenie úrovne rizika,

- Hodnotenie rizík – proces porovnania výsledkov analýzy rizík s kritériami rizík na určenie, či je riziko prijateľné.

Význam hodnotenia účinnosti bezpečnostného spočíva predovšetkým v hodnotení zraniteľných miest a ochranných opatrení, ktoré je súčasťou analýzy rizík. Pri kvantitatívnom hodnotení účinnosti bezpečnostných opatrení sa používa matematický model stráženého priestoru a vzhľadom na výpočtovú zložitosť sa na získavanie výstupných hodnôt používa špecializovaný softvér. Vzhľadom na náročnosť postupu, je typické použitie tejto architektúry predovšetkým v oblasti jadrovej bezpečnosti. Napríklad v [1], je zadefinovaný vzťah pre riziko R :

$R = P_A . [1-(P_E)] . C,$

kde P_A je pravdepodobnosť útoku daná hrozbami a zraniteľnosťami (často sa používa hodnota 1) , P_E je pravdepodobnosť účinnosti systému (pravdepodobnosť prerušenia a pravdepodobnosť eliminácie narušiteľa) a C je hodnota aktíva / veľkosť dopadu.

1.1 ÚČINNOSŤ A VYVÁŽENOSŤ BEZPEČNOSTÝCH SYSTÉMOV

Uviesť definíciu účinnosti bezpečnostného systému môže byť prekvapivo veľmi zložité. Podľa technických definícií je účinnosť bezrozmerné číslo, ktoré vyjadruje ako blízko k ideálnemu procesu prebieha proces v hodnotenom systéme alebo zariadení. Ideálny proces má účinnosť 100 %.[3] Účinnosť bezpečnostného systému môže potom analogicky vyjadrovať ako blízko majú reálne procesy v bezpečnostnom systéme k ideálnym procesom, pričom ideálnymi procesmi sa rozumejú procesy, ktoré úplne eliminujú riziká (alebo ich znižujú na akceptovateľnú úroveň), ktoré boli identifikované a proti ktorým bol bezpečnostný systém projektovaný. Pre vyjadrovanie účinnosti bezpečnostného systému však budeme používať špecifické výstupné parametre, ktoré sú vytvorené ad hoc pre tento účel a ich definovanie je jednoznačné.

Vyváženosťou bezpečnostného systému sa rozumie taká vlastnosť bezpečnostného systému, pri ktorej je bezpečnostný systém dostatočne účinný a má rovnomernú vnútornú štruktúru. Hľadanie vyváženého bezpečnostného riešenia znamená hľadanie bezpečnostného riešenia, ktoré by bolo účinné, ale ekonomicky efektívne. Bezpečnostný systém teda chráni proti útokom vedeným z rôznych strán a rôznymi spôsobmi približne rovnako a vždy účinne.

Ak by bezpečnostný systém nechránil približne rovnako proti rôznym útokom (niektoré miesta by boli oveľa lepšie chránené ako iné), hoci by aj chránil vždy účinne, tak by dochádzalo k určitým ekonomickým stratám pri investovaní do bezpečnosti, pretože narušiteľ by pravdepodobne selektívne vybral cestu s najmenším odporom a účinnejšiu ochranu by obišiel.

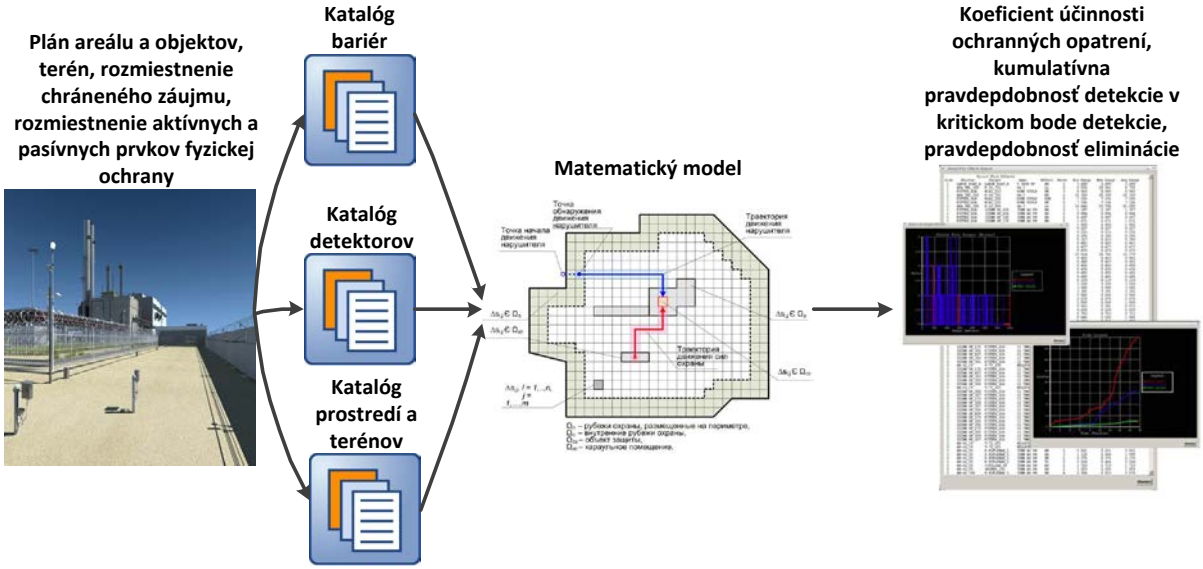
2 VÝSTUPNÉ PARAMETRE

V tejto časti sa budeme venovať štyrom najdôležitejším parametrom, ktoré sú podstatou existujúcich modelov popísaných v domácich a zahraničných prameňoch :

- Minimálna doba zdržania,
- Koeficient účinnosti ochranných opatrení,

- Kumulatívna pravdepodobnosť detekcie,
- Kritický bod detekcie.

Obr. 2 znázorňuje schému modelovania bezpečnostných systémov a jej jednotlivé časti, akú sú vstupné a výstupné parametre, katalógy rôznych prvkov a matematický model.



Obrázok 2 Schematické znázornenie modelovania bezpečnostných systémov

2.1 MINIMÁLNA DOBA ZDRŽANIA

Minimálna doba zdržania je najkratší kumulatívny čas, ktorý potrebuje narušiteľ na dosiahnutie cieľa pri prekonávaní jednotlivých ochranných prvkov systému alebo pri prekonávaní vzdialeností jednotlivých priestorov.[9] Ak použijeme štandardný sieťový graf, tak minimálna doba zdržania je dĺžka najkratšej cesty v grafe.

Aj keď dĺžka najkratšej cesty sa môže porovnať s časom nevyhnutným pre vykonanie zásahu, minimálna doba zdržania má veľmi malú výpovednú hodnotu o účinnosti bezpečnostného systému, pretože neobsahuje vôbec informáciu o detekcii narušiteľa (ku ktorej nemusí dôjsť).

2.2 KOEFICIENT ÚČINNOSTI OCHRANNÝCH OPATRENÍ

Jedným z významných teoretických východísk je používanie výstupnej veličiny nazvanej koeficient účinnosti ochranných opatrení, ktorý závisí priamoúmerne od času prekonávania bezpečnostného systému od momentu detekcie narušiteľa a nepriamoúmerne od celkového času zásahu zásahovej jednotky (fyzickej ochrany alebo zásahovej jednotky). Termín pochádza z [3],[4].

Čas prekonávania bezpečnostného systému potom pozostáva z nasledujúcich časových údajov :

- čas prekonania všetkých pasívnych prvkov ochrany od momentu detekcie,
- celkový čas potrebný na presun narušiteľa k chránenému záujmu od momentu detekcie,
- celkový čas potrebný na únik narušiteľa.

Za časový začiatok sa berie moment detekcie narušiteľa v stráženom priestore. Celkový čas zásahu zásahovej jednotky pozostáva z nasledujúcich časových údajov :

- Čas vyhlásenia poplachu,
- Čas verifikácie napadnutia,
- Čas presunu na miesto zásahu,
- Čas zásahu proti narušiteľovi.[3]

Takto zadefinovaný koeficient účinnosti ochranných opatrení je významnou veličinou, ktorá zo svojej podstaty garantuje účinnosť bezpečnostného systému v tom zmysle, že zásahová jednotka bude mať dostatočný čas na príchod a vykonanie zásahu pred tým, ako narušiteľ dokončí útok a opustí strážený priestor.

Hoci je koeficient účinnosti ochranných opatrení užitočný výstupný parameter, vo forme jednoduchého vzorca je jednorázovo použiteľný pre hodnotenie účinnosti takého bezpečnostného systému, ktorý má chránený záujem koncentrovaný v jedinej bezpečnostnej zóne a aby bola prakticky aplikovaný, musí sa uvažovať s dvoma podmienkami :

- trasa narušiteľa musí byť presne známa pre potreby určenia momentu detekcie,
- musíme byť schopný určiť na tejto ceste miesto detekcie.

Splniť tieto dve podmienky je v praxi jednoduché. Trasa narušiteľa (cesta cez sieťový graf) musí byť presne známa, aby bolo možné vykonať výpočet, pričom v reálnych situáciách do jedinej zóny vedie veľmi veľké množstvo rôznych ciest. S využitím výpočtovej techniky nie je však žiadny problém nájsť všetky možné trasy, vypočítať pre všetky trasy koeficient účinnosti ochranných opatrení a určiť minimálnu hodnotu, spomedzi týchto hodnôt, ako výslednú hodnotu.

Pre potreby výpočtu koeficientu je nevyhnutné stanoviť na každej ceste miesto detekcie, čo znamená zadefinovať minimálnu pravdepodobnosť detekcie, pri ktorej sa dá hovoriť o praktickej istote detekcie (napr. 95 percent, čo nie je problém pri existujúcich technologických možnostiach detektorov dosiahnuť). Túto pevnú hranicu by bolo možné samozrejme dosiahnuť jednorázovo alebo kumulatívne (viacerými detektormi v jednej alebo viacerých zónach).

Hoci táto detekcia nie je úplne stopercentná, v praktických podmienkach ju možno považovať za spoľahlivú. Ani prielomové časy rôznych mechanických zábranných prostriedkov nie sú úplne stopercenté, nakoľko rôzne bezpečnostné zámky sa teoreticky dajú otvoriť s použitím špeciálnych techník, ale podobne ako v prípade detektorov, tento problém zostáva skôr v teoretickej ako praktickej rovine a patrí do oblasti hodnotenia spoľahlivosti, nie účinnosti bezpečnostných systémov.

Je nesporné, že bez určenia takejto pevnej hranice by koeficient účinnosti ochranných opatrení stratil úplne význam v hodnotení účinnosti bezpečnostných systémov. Koeficient účinností ochranných opatrení, ktorý by napríklad vychádzal z celkového času prekonávania všetkých pasívnych prvkov, by bol ľahko vypočítateľný ale pomerne nezaujímavý údaj, nakoľko by zahrňoval aj čas, v ktorom narušiteľ vniká do stráženého priestoru alebo sa v ňom dokonca pohybuje, ale nie je vyhlásený poplach.

Je zrejmé, že jednoduchým spôsobom ako zvýšiť koeficient účinnosti ochranných opatrení je koncentrovať chránený záujem približne v strede systému a vysunúť detekčné prvky čo najbližšie k okoliu objektu, teda na okraj systému. Koncentrácia chráneného záujmu v centrálnej zóne môže však byť v systémoch na

ochranu majetku a osôb z praktických dôvodov nemožná, vysúvanie detekčných prvkov ďalej od stredu môže byť veľmi nákladné pre rozsiahle bezpečnostné systémy, keďže obvod narastá.

2.3 KUMULATÍVNA PRAVDEPODOBNOSŤ DETEKCIE

Kumulatívna pravdepodobnosť detekcie určuje celkovú pravdepodobnosť, že nastane detekcia narušiteľa pri jeho prechode stráženým priestorom. Keďže detekcia narušiteľa dvomi rôznymi detekčnými prvkami v dvoch rôznych zónach sú nezávislé javy, kumulatívnu pravdepodobnosť detekcie možno matematicky definovať ako pravdepodobnosť prieniku náhodných udalostí.

S používaním kumulatívnej pravdepodobnosti detekcie súvisia podobné problémy ako a používaním koeficientu účinnosti ochranných opatrení, predovšetkým musí byť známa trasa postupu narušiteľa, aby sa dala kumulatívna pravdepodobnosť vôbec vypočítať. Podobne ako celkový čas zdržania, aj kumulatívna pravdepodobnosť detekcie má pre hodnotenie účinnosti bezpečnostných systémov samozrejme malý význam.

2.4 KRITICKÝ BOD DETEKCIE

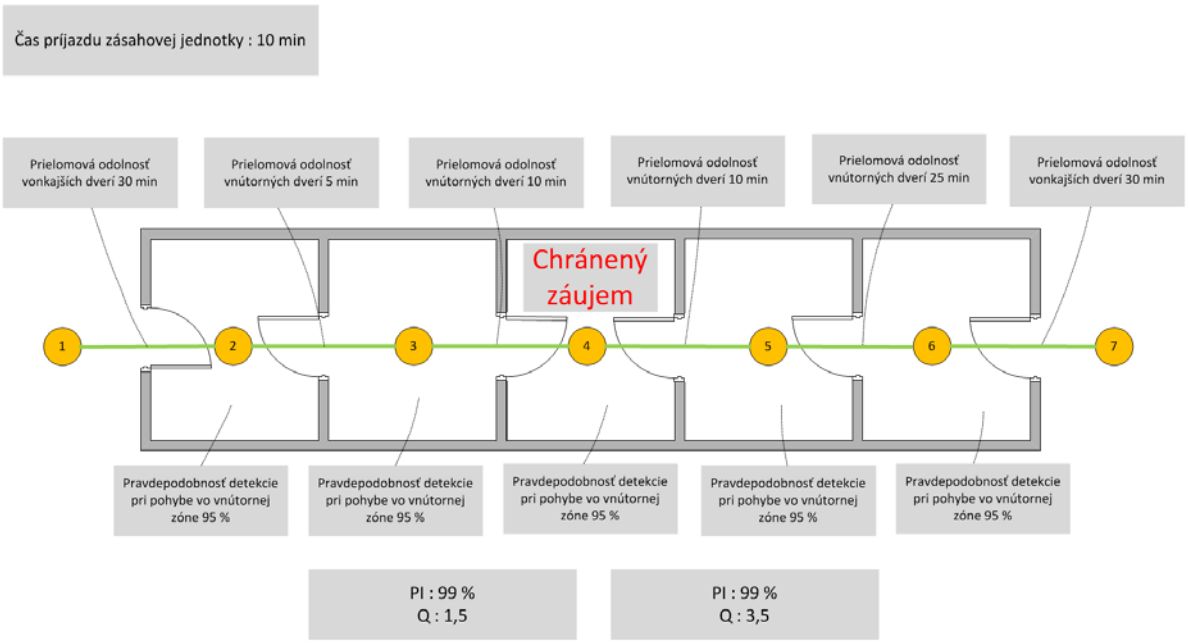
Myšlienka kritického bodu detekcie je jednoduchá a spočíva v tom, že na zvolenej ceste narušiteľa cez strážený priestor sa nájde bod, pre ktorý platí, že ak dôjde k detekcii až za týmto bodom, narušiteľ stihne úspešne dokončiť útok a opustiť priestor pred príchodom zásahovej jednotky.[9]

Skúmanie polohy samotného kritického bodu detekcie nemá význam, ale zaujímavý je údaj o kumulatívnej pravdepodobnosti detekcie narušiteľa do jeho príchodu na kritický bod detekcie. Pritom platí, že táto hodnota musí byť veľmi vysoká a naopak detekcia za týmto miestom je považovaná za neefektívnu.

3 KOMPARÁCIA VÝSTUPNÝCH PARAMETEROV

Stručný rozbor ukázal, že najväčší význam majú dva výstupné parametre – koeficient účinnosti ochranných opatrení a pravdepodobnosť prerušenia. Keďže obidva parametre sú podobné, je zaujímavé ich vzájomne porovnať. Koeficient účinnosti ochranných opatrení sa počíta takým spôsobom, že sa od začiatku cesty vyhľadáva bod detekcie a potom sa vypočíta čas zdržania na zvyšku cesty až do konca a ten sa vydelí časom zásahu. Kumulatívna pravdepodobnosť detekcie sa počíta naopak od konca cesty, od ktorého sa odčíta čas zásahu a potom sa vypočíta kumulatívna pravdepodobnosť detekcie až na začiatok cesty.

Ako ukazuje ilustračný príklad na obr. 3, medzi hodnotami obidvoch koeficientov nemusí byť žiadna korelácia, hoci je to prejavom nevyváženosti bezpečnostného systému. Koeficient účinnosti ochranných opatrení je na obr. 3 označený *Q* a pravdepodobnosť prerušenia *PI*. Z toho vyplýva potreba skúmať vzťah medzi hodnotou chráneného záujmu a obidvomi výstupnými parametrami pre každú bezpečnostnú zónu ako súčasť hodnotenia vyváženosti bezpečnostného systému.



Obrázok 3 Porovnanie koeficientu účinnosti ochranných opatrení a pravdepodobnosti prerušenia

4 ZÁVER

Z vykonanej komparácie výstupných parametrov používaných pri hodnotení účinnosti bezpečnostných systémov vyplýva, že za najlepšie parametre možno označiť koeficient účinnosti ochranných opatrení a pravdepodobnosť prerušenia. Vzhľadom na uvedené fakty týkajúce sa daných parametrov by sme však jednoznačne odporúčali používať tieto dva výstupné parametre v praktických aplikáciách spoločne, pretože najviac praktických výstupov sa dá vyvodiť až z kombinácie obidvoch hodnôt.

LITERATÚRA

[1] GARCIA M.L. 2008. The Design nad Evaluation of Physical Protection Systems : Sandia National Laboratories. 351 s. ISBN 978-0-7506-8352-4

[2] HAMMER C. 1992. Tactics and Techniques for bypassing alarms and defeteing locks: Paladin Press. 107 s. ISBN 0-87364-686-6

[3] LOVEČEK T. 2009. Systémy ochrany majetku a možnosti ich kvalitatívneho a kvantitatívneho ohodnotenia : Habilitačná práca. Žilina.

[4] LOVEČEK T. 2005. Hodnotenie kvality bezpečnostných systémov : Dizertačná práca. Žilina.

[5] MCCRIE R. 2001. Security Operations Management : Butterworth–Heinemann. Woburn. 429 s. ISBN 0-240-80384-1.

[6] PHILLIPS G. 2004. New Vulnerability Assessment Technologies vs the Old VA Tools. New Meets Old. National Security Program Office.

[7] REITŠPÍS J. 2004. Manžérstvo bezpečnostných rizík : Edis. Žilina. 296 s. ISBN 80-8070-328-0

[8] SAVI 4.0, Reference manual, Sandia National Laboratories

[9] Physical Protection of Nuclear Facilities and Materials, Albuquerque, New Mexico, USA

[10] A Risk Assessment Methodology (RAM) for Physical Security. 2005. Sandia Corporation, White Paper.

[11] FM 3-19.30 : Physical Security, 2001, Headquarters, Department of the Army, USA , 317 s.

[12] ISO 31000 : Manažment rizika

Vydanie článku bolo podporené projektom APVV-0471-10.

Článok recenzoval:
prof. Ing. Josef Reitšpís, PhD.