

SLOVENSKÁ ŠTATISTIKA a DEMOGRAFIA

SLOVAK STATISTICS
and DEMOGRAPHY

2/2019

ročník/volume 29

Recenzovaný vedecký časopis so zameraním na prezentáciu moderných štatistických a demografických metód a postupov.

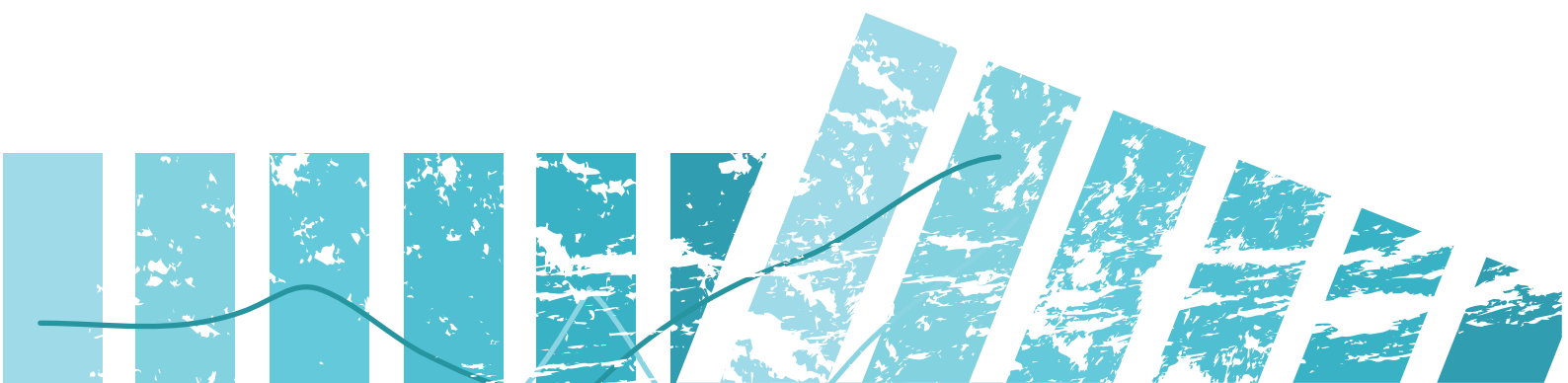
Scientific peer-reviewed journal focusing on the presentation of modern statistical and demographic methods and procedures.

Článok/Article: 7

Typ článku/Type of article: informatívny článok/informative article

Strany/Pages: 70 – 79

Dátum vydania/Publication date: 15. apríl 2019/April 15, 2019



Marek HARGAŠ
Štatistický úrad Slovenskej republiky

ÚLOHA MODERNÝCH ŠTATISTICKÝCH METÓD VO VÝSKUME BEZPEČNOSTI

THE ROLE OF MODERN STATISTICAL METHODS IN SECURITY RESEARCH

ABSTRAKT

Príspevok sa zaoberá štatistickými metódami, ktoré sa využívajú v oblasti bezpečnosti. Ich použitie je dané predovšetkým potrebou identifikovať a vyhodnocovať nástroje bezpečnostného manažmentu a manažmentu rizík aj v spojení s výskumom bezpečnosti. Základný opis používaných štatistických metód sa odvíja od ich zaradenia medzi klasické deterministické metódy a moderné metódy založené na stochastickom základe. Spracovanie zdrojov naznačuje oblasti, kde sa dnes uvedené metódy aplikujú, a vytvára predpoklady na ich detailné preskúmanie vo vzťahu k výskumu bezpečnosti na Slovensku.

ABSTRACT

The contribution deals with the statistical methods that are used in the field of security. Their use is primarily driven by the need to identify and evaluate the tools of security management and risk management also in connection with the security research. The basic description of the statistical methods used is based on their inclusion among the classical deterministic methods and modern methods based on the stochastic principle. The processing of sources suggests the areas where these methods are applied today and creates conditions for their detailed examination in relation to the security research in the Slovak Republic.

KLÚČOVÉ SLOVÁ

bezpečnosť, rizikový manažment, štatistické metódy

KEYWORDS

security, risk management, statistical methods

1. ÚVOD

V súčasnosti pojem bezpečnosti väčšina ľudí vníma výhradne ako subjektívny pocit. Všeobecne môžeme toto subjektívne vnímanie charakterizovať ako vnímanie status quo entity v internom a externom prostredí, resp. ako taký stav, keď sa entita cíti bezpečne. Samozrejme, definícia bezpečnosti sa posudzuje a vymedzuje inak pre individuálny subjekt, inak pre rôzne záujmové skupiny, organizácie a inak pre etniká, štáty a spoločenstvá štátov. Súčasná spoločnosť vníma problematiku bezpečnosti, a to najmä nevojenskej bezpečnosti, pomerne citlivo. Zároveň otázky bezpečnosti formujú správanie entít tak na mikroúrovni, aj na makroúrovni. Formy, metódy, nástroje v oblasti bezpečnosti sú dnes oveľa sofistikovanejšie ako v minulosti, keď sme odvodzovali svoju bezpečnosť v zmysle bezpečnosti štátu v bipolárnom geopolitickom svete (sféry vplyvu USA verzus bývalý Sovietsky zväz).

V príspevku sa budeme venovať klasickým aj moderným štatistickým metódam, ktoré sa využívajú pri výskume bezpečnosti predovšetkým na individuálnej rovine

sekuritizácie, pri skúmaní agregátnych modelov a scenárov vývoja v oblasti bezpečnosti ako aj pri rizikovej analýze. Stručne a všeobecne definujeme predmetné metódy a identifikujeme ich konkrétne použitie.

2. BEZPEČNOSŤ A BEZPEČNOSTNÝ MANAŽMENT

Problém definovania bezpečnosti je, že neexistuje jedna definícia. V súčasnosti sa bezpečnosť poníma multidisciplinárne, a to v dynamickom prostredí, ktoré sa posledné desaťročia dramaticky mení.

Podľa Lasicovej a Ušiaka [7, s. 14] „prehľbovanie skúmania bezpečnosti nastáva so zmenou analytických rovín. O bezpečnosti môžeme hovoriť z globálneho, regionálneho, subregionálneho, lokálneho, skupinového a individuálneho hľadiska. Každá analytická rovina má svoju sociálnu štruktúru, vlastné režimové vzorce, ale výsledok môže byť závislý aj od metodologického prístupu, teda či budeme pri skúmaní ako metodologický aparát využívať rôzne teórie, nimi rozpracované paradigmy, alebo modely a simulácie, vytvorené ako simulakrum na spracovanie kvantitatívnych a kvalitatívnych dát.“

Riziko je súčasťou našich životov. Bez rizika neexistuje žiaden systém v ktorom fungujeme ako entita, či spoločnosť. Preto je potrebné vedieť s rizikami existovať, byť schopný riziká identifikovať, analyzovať, evidovať, kategorizovať, rýchlo na riziká reagovať a následne ich mitigovať respektíve, ak je to možné, ich eliminovať. Na to slúži rizikový alebo bezpečnostný manažment.

Bezpečnostný manažment môžeme chápať ako proces identifikácie, analýzy a odpovede na rizikové faktory počas životného cyklu entity v zmysle jej záujmov a cieľov. Vhodný bezpečnostný manažment skôr zahŕňa proaktívne riadenie budúcich situácií ako reaktívne riadenie [12]. Bezpečnostný manažment má niekoľko fáz, najčastejšie sa rozlišujú fáza identifikácie, fáza vyhodnotenia rizika, fáza riadenia rizika a fáza monitorovania.

Tak ako definícia bezpečnosti aj problematika bezpečnostného manažmentu je extenzívna a komplexná. Neexistuje žiadny generálny prístup, ako realizovať bezpečnostný manažment. Výber vhodnej metódy záleží na viacerých kritériách, napríklad obsahu a cieľoch bezpečnostnej analýzy, prostredí bezpečnostného aktéra, a veľmi dôležitým aspektom pri metódach analýzy bezpečnostných rizík je kvalita a kvantita informácií [6].

Optimálna riziková analýza je založená na analýze historických dát vo vzťahu k sledovanému objektu. Po štatistickom zovšeobecnení a spracovaní empirických dát môžeme následne určiť pravidelnosť výskytu udalostí, ktoré môžu byť definované ako rizikové. Práve tu prichádzajú do úvahy štatistické metódy, ktoré objektivizujú udalosti a okolnosti, ktoré dokážeme následným spracovaním použiť pre manažment rizika a/alebo bezpečnosti. Moderné štatistické metódy dokážu vyhodnocovať aj s neistotami a nepresnosťami v inputovaných dátach [9].

3. ŠTATISTICKÉ METÓDY V RIZIKOVEJ ANALÝZE

Štatistické metódy, ktoré dokážu pracovať aj s nepresnými dátami a ktoré sa používajú v rizikovej analýze, rozdeľujeme na (1) klasické deterministické metódy a (2) moderné metódy založené na stochastickom základe.

Do prvej skupiny patrí predovšetkým analýza stromu udalostí (Event Tree Analysis, ETA), analýza stromu poruchových javov (Fault Tree Analysis, FTA), analýza príčin a dôsledkov (Failure Modes and Effects Analysis, FMEA), analýza spôsobov a dôsledkov kritickosti porúch (Failure Mode, Effects, and Critical Analysis, FMECA).

V druhej skupine ide najmä o simuláciu Monte Carlo, metódu časových radov (TSM), metódu Markovovho reťazca, metódu scenárov, regresnú analýzu, analýzu neurónových sietí a Bayesiánsku metódu.

3.1 KLASICKÉ DETERMINISTICKÉ ŠTATISTICKÉ METÓDY

Predmetné klasické metódy sa dajú primerane použiť v oblasti skúmania bezpečnosti a jej vojenskej aj nevojenskej stránky. Obzvlášť sa hodia na skúmanie bezpečnostných otázok na úrovni organizácie, na individuálnej úrovni a na úrovni menších entít. Bohato sa používajú pri sekuritizácii aj v oblasti energetiky a environmentálnych hrozieb. Spravidla sa týkajú bezpečnostných analýz a prognóz malých entít v úzko definovanom rozsahu. Tieto metódy sa skôr používajú pri riadení rizík ako pri výskume bezpečnosti.

Analýza stromu udalostí (ETA)

Ide o kauzálnu induktívnu analytickú techniku, ktorá poukazuje na možné výsledky vyplývajúce z náhodných udalostí. Definuje proces a jeho možné udalosti, ktoré vedú k novej nehode. Analýza stromu udalostí dokáže identifikovať potenciálne rizikové scenáre a sekvencie v komplexnom systéme. Dizajn a procedurálne slabosti sú identifikované v samotnom procese, pričom podľa Marvina Rausanda a Arljota Hoylanda [10] táto metóda vie definovať pravdepodobnosti rôznych výsledkov z rôznych udalostí. ETA svoje empirické dáta zobrazuje pomocou grafického logického modelu v kauzalite udalostí – výsledok s definíciou pravdepodobnosti incidentu.

Pôvodne bola táto metóda vyvinutá na žiadosť jadrového priemyslu po havárii v elektrárni Three Mile Island.

Postup pri analýze pomocou ETA by mal podľa [10, s. 109] zahŕňať 6 nasledujúcich krokov: (1) identifikácia relevantnej závažnej východiskovej (náhodnej) udalosti, ktorá môže viesť k nechceným následkom, (2) identifikácia bezpečnostných funkcií, ktoré sú určené na to, aby sa vyrovnali s východiskovou udalosťou, (3) vytvorenie stromu udalostí, (4) popis možných následkov, (5) výpočet pravdepodobností/frekvencie identifikovaných následkov, (6) zostavenie a prezentácia výsledkov analýzy.

Metóda má praktické využitie pri definovaní bezpečnostných bariér a opatrení napr. v energetike, v oblasti ochrany životného prostredia. Použitie metódy je najmä pri rizikovej analýze technologických, energetických a environmentálnych systémoch a pri identifikácii v ochrane takýchto systémov [10], ako aj pri riadení bezpečnosti.

Analýza stromu poruchových javov (FTA)

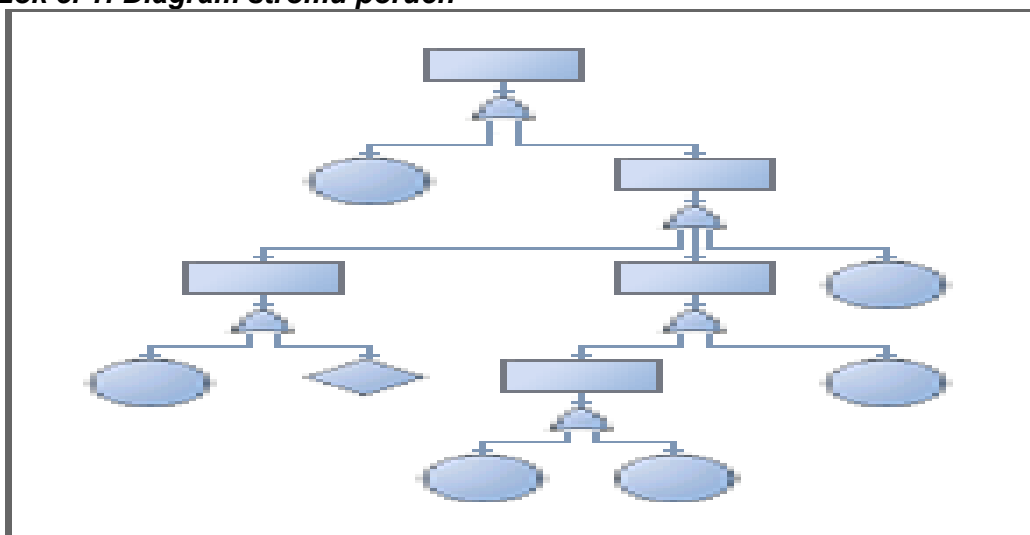
Analýza stromu poruchových javov je analytická technika, ktorá sa používa na vyhodnotenie pravdepodobnosti zlyhania v komplikovaných systémoch. Jej cieľom je vypočítať pravdepodobnosti zlyhania celého systému a definovať spôsoby mitigácie

rizika. Táto metóda identifikuje, modeluje a vyhodnocuje vzájomné vzťahy udalostí, napr. zlyhanie, neočakávané udalosti a stavy, neplánované udalosti a stavy.

Ako uvádza [1], metóda bola prvýkrát predstavená H.A. Watsonom z Bellových laboratórií v rámci štúdie pre U.S. Air Force okolo roku 1961, konkrétne pri vyhodnotení odpaľovacieho systému pre medzinárodné balistické rakety Minuteman. Nasledovalo použitie metódy v spoločnosti Boeing v 70. rokoch. K rozšíreniu metódy napomohlo aj jej použitie pri zaistení adekvátnej bezpečnosti dizajnu po havárii vesmírnej lode Challenger v roku 1986.

Nástroje FTA vyhodnocujú komplex systémov, identifikujú udalosti, ktoré spôsobujú neželanú udalosť, skúmajú bezpečnosť, spoľahlivosť, nedostupnosť a poruchové súvislosti [1]. Predmetná analýza je deduktívna a poskytuje zhodnotenia rizík aktéra. Model je grafický, zobrazuje vzťah príčina-následok s vyjadrením pravdepodobností. Vizualizácia FTA modelu v softvéri Visio Professional je zobrazená na obrázku č.1.

Obrázok č. 1: Diagram stromu porúch



Zdroj: Visio Professional 2019, Visio Standard 2019, [tps://support.office.com/cs-cz](https://support.office.com/cs-cz)

Do 70. rokov minulého storočia bola FTA významne využívaná strategickými ozbrojenými silami USA, ako aj NASA. Dodnes sa často využíva aj pri analýze rizík zbraňových systémov.

Analýza príčin a dôsledkov (FMEA)

Analýza príčin a dôsledkov je analýzou príčin a dôsledkov konkrétneho technického systému. Definuje a analyzuje dotknuté riziká, klasifikuje ich podľa veľkosti ohrozenia systému a podľa pravdepodobnosti výskytu predmetných ohrození. Pri tejto metóde sa tiež analyzuje história podobných produktov a skúseností. Metóda bola vyvinutá pre vojenskú oblasť a až neskôr sa rozšírila aj do privátnej oblasti. Proces použitia FMEA pozostáva z 5 krokov:

1. Identifikácia potenciálnej škody a následkov škody – analýza funkčných požiadaviek a ich efekt pri identifikácii všetkých typov škôd (napríklad zoznam všetkých typov škôd na jednotlivé funkcie systému).

2. Určenie rozsahu škody – rozsah je definovaný ako vážnosť následku škody pri škodovej udalosti. Vytvára sa rating škôd a priraduje sa klasifikácia rizika resp. škody podľa vážnosti (napr. 1 – bez rizika,, 10 – veľmi vysoké riziko).

3. Meranie pravdepodobnosti kedy škoda nastane – ide o meranie príčin každej udalosti, keď vzniká škoda. Snahou je štandardizovať vecný a časový aspekt jednotlivých kategorizovaných škôd. (napr. 1- nedokumentovaný incident,, 9 – vysoké riziko – pravidelná dokumentovaná škoda, chyba).

4. Detekcia škody – identifikovaná škoda je ustálená a determinujú sa mitigačné a eliminačné opatrenia. Nastavuje sa detekčný systém. (napr. 1 – chyba sa zachytí 100 % na testovacom rozhraní, ..., 9 – chybu neodhalí ani jeden kontrolný systém).

5. Definícia rizikového prioritného čísla (RPN) – RPN sa kalkuluje na konkrétny proces oproti rizikovej pravdepodobnosti a závažnosti a detekcie škody.

$$RPN = \text{závažnosť} \times \text{pravdepodobnosť výskytu} \times \text{detekcia škody} [4]$$

Keďže ide o systémový prístup, metóda má široké spektrum použitia, záleží na druhu analyzovaného systému a definovaných cieľoch. Analýzu príčin a dôsledkov v oblasti bezpečnosti štandardne využíva agentúra NASA od havárie raketoplánu Challenger. Predmetné rizikové analýzy majú spracované azda všetky armády na svete, vlády, ako aj veľké korporácie.

Postup analýzy spôsobov a dôsledkov kritickosti porúch (FMECA)

Tento postup slúži na systematickú identifikáciu potenciálnych škôd a porúch, ktoré majú efekt na koncových používateľov systému. V princípe je metodika analýzy podobná FMEA, ale dôraz sa kladie na kvalitu na konci procesu. Analýza umožňuje identifikovať bezpečnostné riziká a zodpovednosti v skúmanej oblasti a dá sa použiť aj na identifikáciu situácií kedy a v ktorých bodoch alebo situáciách systém nevyhovuje regulácii.

3.2 MODERNÉ METÓDY ZALOŽENÉ NA STOCHASTICKOM ZÁKLADE

Predmetné moderné štatistické metódy majú veľmi dobré uplatnenie pri skúmaní bezpečnosti, či na úrovni individuálnej bezpečnosti, ale významne sa podieľajú aj na príprave strategických bezpečnostných konceptov. Využívajú sa najmä pri analyzovaní väčších, sektorových tém.

Metóda Monte Carlo

Podľa [2, 11] metóda Monte Carlo je stochastickou metódou riešenia matematických a iných problémov s využitím modelovania náhodných veličín. Základnou myšlienkou je využitie náhody na deterministické riešenie nastoleného problému. Metóda je založená na hľadaní hodnoty veličiny X , ktorá súvisí s istým náhodným procesom. Tento proces modelujeme na počítači, čím získame realizácie náhodnej veličiny X . Pomocou realizácií veličiny X odhadujeme s určitou presnosťou hodnotu pôvodnej hľadanej veličiny X . Výpočet pomocou danej metódy zahŕňa nasledujúce kroky: (1) generovanie náhodného čísla y_i s rovnomerným rozdelením na intervale (0,1), (2) transformáciu na náhodné čísla z_i s potrebným rozdelením, (3) pomocou náhodných čísel z_i sa buď priamo počítajú odhady charakteristík náhodnej veličiny X , alebo sa počítajú pomocou vhodného algoritmu hodnoty x_i , (4) získané výsledky sa štatisticky spracujú. Na vyhodnotenie simulácií sa často používajú štatistické metódy, ako priemer, smerodajná odchýlka, modus, medián. Aby sme dosiahli potrebnú presnosť, je potrebné mnohonásobné

opakovanie simulácie. Súčasne s odhadom neznámej hodnoty je dôležité i určenie presnosti odhadu.

Metóda Monte Carlo bola navrhnutá a využitá po prvýkrát v Spojených štátoch amerických pri vývoji atómovej bomby počas druhej svetovej vojny. Neskôr sa používala pri riešení fyzikálnych problémov, do tej doby prakticky neriešiteľných a jej použitie sa rozširovalo s rozvojom počítačovej techniky a teórie modelovania na oblasť techniky, ekonomiky, riadenia dopravy a pri riešení problémov v samotnej matematike.

Metóda Monte Carlo má široké využitie od simulácie experimentov až po riešenie diferenciálnych rovníc. Metódu je možné využiť predovšetkým všade tam, kde je riešenie problému určitým spôsobom závislé od pravdepodobností. Dobré výsledky má pri projektovaní v oblasti neznámej budúcnosti, ako aj pri iných podobných metódach, záleží na kvalite odhadov a vhodne zvolenom rozsahu skúmania (integrované maximá). Táto metóda má dobré využitie v prognózovaní bezpečnostného prostredia. Vo vojenskom sektore sa používa pri simulácii vojnových stavov v tzv. vojnových hrách, pri analýze vojenskej komunikácie a v oblasti leteckej prevádzky.

Metódy analýzy časových radov

Analýza časových radov je založená na údajoch o štatistickom znaku usporiadanom v čase a umožňuje definovať trendy interpeláciou (vyrovnávaním) a extrapoláciou (prognózou) a to ako v minulosti, tak aj v budúcnosti. Aj pri tejto pomerne často využívannej analýze je potrebné mať k dispozícii čo najviac koherentných údajov definovaných v čo najdlhšej časovej perióde. Trendy sú spravidla stúpajúce, klesajúce, môžu oscilovať, prípadne náhodne kolísať. V praxi poznáme stacionárne a nestacionárne modely. Pri stacionárnom (deterministickom) modeli analyzujeme koherentné údaje na konštantnej úrovni, chronologicky usporiadané. Stacionárny model analyzuje iba minulosť. Nestacionárne modely založené na stochastickom princípe ukazujú trendy a predpovede. Metóda časových radov je dobre a pomerne analyticky definovaná v [13].

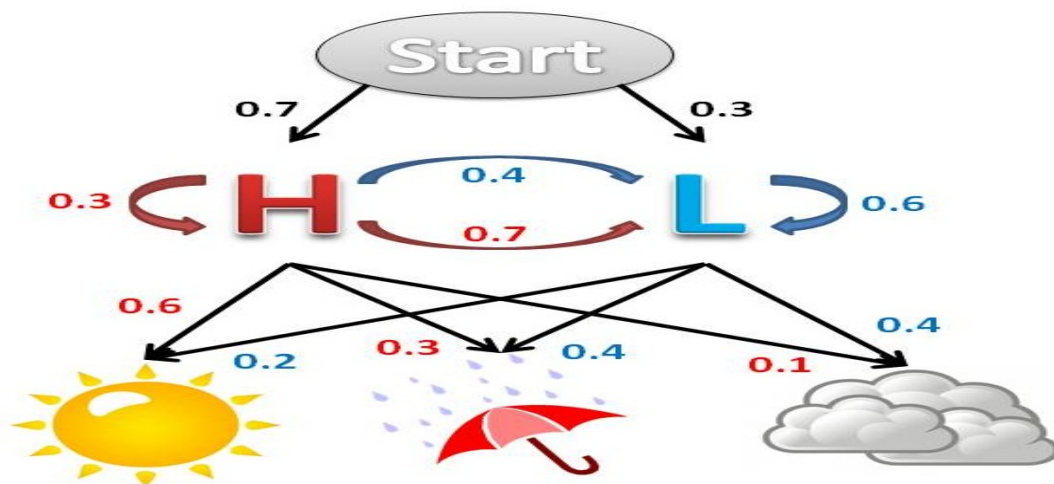
Vo vojenskom sektore sa táto metóda pomerne často využíva od analýzy hospodárnosti výdavkov na vojenský sektor až po definíciu dopytu na muníciu delostreleckých systémov.

Metóda Markovovho reťazca

Metóda Markovovho reťazca je založená na modelovaní systémov s jasne určenými stavmi a prechodmi. Podľa Lipku [8] Markovov predpoklad bol založený na myšlienke, že pravdepodobnosť stavu závisí len od predchádzajúceho stavu a nie od jeho prechodu, alebo naopak, pravdepodobnosť prechodu do nasledujúceho stavu závisí výlučne od súčasného stavu. Markovov model umožňuje pomerne jednoducho graficky zobrazíť stavy a ich zmeny vo vzťahu k pravdepodobnosti, ako môžeme vidieť na obrázku č. 2 v prípade počasia.

V bezpečnostnom a vojenskom sektore sa metóda používa napríklad na definíciu bezpečnostných a vojenských procesov, plánovanie personálnej dynamiky, ale aj prognózovanie pravdepodobnosti prežitia vo vzdušnom boji atď.

Obrázok č.2: Jednoduchá ukážka Markovovho modelu



Zdroj: <http://guizzetti.ca>

Metóda scenárov

Scenár je model, ktorý opisuje budúci vývoj a stav ohraničeného systému. Pri opisovaní budúceho stavu sa spravidla používajú tri scenáre – optimistický, realistický a pesimistický. Táto analýza sa využíva pri prognózovaní vývoja ucelených systémov. Daný systém musí byť čo najlepšie analyzovaný a štandardizovaný. Na tento účel sa používajú rôzne, aj predtým uvedené analýzy ako STEP, SWOT, BIAS, Markovov model, analýza Monte Carlo a, samozrejme, ekonomické a bezpečnostné analýzy. Táto metóda sa významne využíva v definovaní geopolitických scenárov. Proces analýzy scenárov zahŕňa: 1. definovanie problému, 2. analýzu a zhromažďovanie dát, 3. zafixovanie overených premenných, 4. vytvorenie scenárov a 5. použitie najvhodnejšieho scenára na plánovanie.

Metóda scenárov má dobré uplatnenie pri skúmaní bezpečnosti vo vojenskom aj nevojenskom sektore. Metóda využitia vojenských, obranných a bezpečnostných scenárov, dokonca aj v oblasti nevojenských operácií, na úrovni taktickej aj strategickej, je základ vojenského prognózovania a strategického plánovania. Pomerne dobrý rozsah použitia metódy scenárov možno nájsť na webovej stránke NATO.

Regresná a korelačná analýza

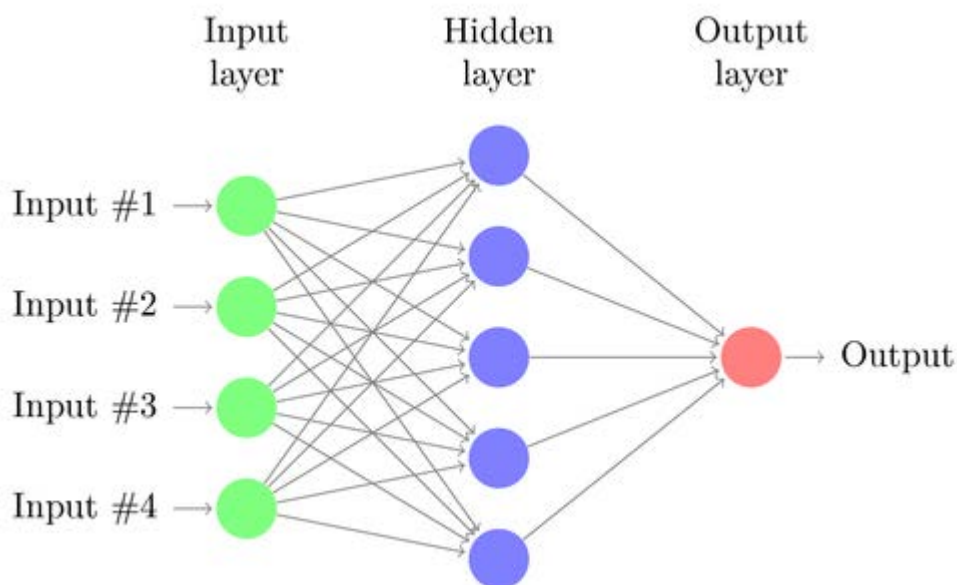
Základom regresnej a korelačnej analýzy je charakterizovať vzájomné vzťahy medzi premennými. Jej úlohou je matematicky definovať tento vzťah. Metóda sa používa na predikciu a predpovede a spracovanie tejto témy. Regresná analýza sa delí na jednoduchú a viacnásobnú. Veličiny sú vzájomne štatisticky korelované, pritom nepoznáme typ a konštantu funkcie, ktorú dodatočne určujeme na podklade empiricky zistených (odmeraných) údajov. Toto riešenie je regresná analýza, tesnosť empirickej závislosti korelovaných veličín od štatisticky vyhodnoteného funkčného vzťahu nazývame korelačná analýza. V rámci regresnej analýzy používame viaceré modely a techniky, ako lineárna a nelineárna regresia, interpolácia a extrapolácia, priestorová regresná analýza, harmonická analýza, lineárna a nelineárna korelácia, atď.

Táto metóda sa pomerne často používa pri skúmaní otázok v oblasti bezpečnosti v oblasti hospodárskych vplyvov a implikácii na bezpečnosť, na predikovanie rôznych situácií, napr. predikovanie dopytových modelov pre vojenské civilné stavy a podobne.

Analýza neurónových sietí

Základnou vlastnosťou neurónových sietí je schopnosť abstrakcie medzi vstupnými a výstupnými hodnotami. Neurónová sieť je odvodená, resp. zostavená podľa štruktúry nervového systému. Je nelineárna, vie sa adaptovať a sieť sa môže meniť podľa potreby výstupov. Užitočnosť neurónovej siete je definovaná schopnosťou abstrakcie a učenia sa. Pre potreby štatistického zisťovania, aproximácie, kategorizácie, plánovania a prognózovania má veľkú výhodu, pretože dokáže spracovať obrovské množstvo dát a dokáže vyberať, prepájať a analyzovať dokonca aj neštruktúrované dáta a časové rady, prípadne siete vedú simultánne realizovať viacero štatistických procesov.

Obrázok č. 3: Opis neurónových sietí



Zdroj: <http://www.texample.net>

Model neurónových sietí sa významne podieľa na prognózovaní v oblasti obranného sektora pri predikcii bojových simulácií, modelov spravodajských situácií a riešení, v oblasti umelej inteligencie, v oblasti bezpečnostného sektora a predikcie fungovania zbraňových systémov.

Bayesova metóda

Je to štatistická metóda na základe bayesovskej pravdepodobnosti, postavená na Bayesovej teoréme, ktorá opisuje ako sa ovplyvňujú dve opačne podmienené pravdepodobnosti. Je to pomerne nová koncepcia, ktorá však vychádza zo starej teórie z 18. storočia. Bayesova teoréma zavádza do výpočtu prognóz určitú subjektivitu a z tohto dôvodu sa vedú odborné spory s frekventistami, ktorí považujú Bayesovu metódu za subjektívnu.

Bayesova veta definuje súvislosť podmienenej pravdepodobnosti $P(A/B)$ a inverznej podmienenej pravdepodobnosti $P(B/A)$ a vyjadruje ich vzťah.

$$P(A/B) = \frac{P(B/A) P(A)}{P(B)}$$

Podmienená pravdepodobnosť $P(A/B)$ je definovaná ako pravdepodobnosť javu A v priestore javu B . Metóda dokáže spresňovať pravdepodobnosť hypotéz v zmysle nových skutočností, kde pravdepodobnosť vyjadruje stupeň istoty v udalosť, ktorá sa môže zmeniť s novou informáciou skôr ako pri zmene hustoty alebo frekvencie [14]. Zjednodušene, metóda vypočíta a aktualizuje pravdepodobnosti po získaní nových skutočností a dá sa dobre použiť pri odhade parametrov aj vo veľkých štatistických modeloch.

V bezpečnostnej oblasti sa bayesovské modely používajú v celom rozsahu skúmania bezpečnosti, najmä v oblasti riadenia bojových konfliktov. Výrazne sa podieľajú na technikách vojenského spravodajstva, v strategickom plánovaní, používajú sa na konkrétne, analytické situácie, ako napr. na prognózovanie konkrétnych zranení vojakov v konfliktných situáciách a miestach.

4. ZÁVER

Hoci je bezpečnosť multidisciplinárna kategória a neexistuje jednotný prístup k jej definícii a výskumu, štatistické metódy majú široké použitie pri výskume vedeckých otázok v tejto kategórii. Tak ako aj v iných disciplínach aj v oblasti bezpečnosti vieme definovať exaktné štatistické metódy výskumu len na mikroúrovni – na úrovni výskumu malých entít v úzkom rozsahu výskumu a v stabilnom, nemeniacom sa prostredí. Výskum bezpečnosti v takýchto podmienkach vieme často realizovať prostredníctvom štandardizovaných metód, ako sú riziková analýza, analýza stromu udalostí, analýza stromu poruchových javov, analýza príčin a dôsledkov a postup analýzy spôsobov a dôsledkov kritickosti porúch.

Výskum širších oblastí bezpečnosti, pre väčšie entity a v dynamickom prostredí môžeme realizovať modernými matematicko-štatistickými metódami, ktoré umožňujú definovať pravdepodobnosti a prognózy v širokých súvislostiach a väčšou mierou neistoty. Sú to predovšetkým metódy ako simulácia Monte Carlo, metóda časových radov (TSM), metóda Markovovho reťazca, metóda scenárov, regresná analýza, analýza neurónových sietí a Bayesova metóda.

Najmä moderné matematicko-štatistické metódy v súčasnej dobe, pri masívnom využití prostriedkov informačno-komunikačných technológií, dokážu simulovať bezpečnostné riziká v pomerne širokom bezpečnostnom prostredí a prognózovať vývoje rôznych scenárov. V súčasnosti všetci svetoví významní bezpečnostní aktéri používajú v bezpečnostnom manažmente predmetné metódy. Ich použitie pri manažmente rizika bude, najmä pri zohľadnení zvyšovania výkonnosti informačno-komunikačných technológií, len narastať.

LITERATÚRA

- [1] ERICSON, C.A. II.: Fault Tree Analysis, 17th International System Safety Conference, 1999 [online].
- [2] FABIAN, F. – KLUIBER, Z.: Metoda Monte Carlo a možnosti jejího uplatnění, Praha: Prospektrum, 1998.
- [3] Failure Modes, Effects and Criticality Analysis, Warwick Manufacturing Group School of Engineering, University of Warwick, 2018. [online].
- [4] How to conduct a failure modes and effect analysis. In: A white paper issued by: Siemens PLM Software, 2016, Dostupné na: www.siemens.com/polarion.
- [5] HOFREITER, L.: Bezpečnostné prostredie súčasného sveta. Bačuvčík R., VeRBuM, 2016, ISBN 978-80-87500-79-8.
- [6] KRÁĽOVÁ, M.: Komparácia metód analýzy bezpečnostných rizík. Diplomová práca, Žilinská univerzita, 2006, [online].
- [7] LASICOVÁ, J. – UŠIAK J.: Bezpečnosť ako kategória. Bratislava, Veda, 2013, 264 s., ISBN: 978-80-224-1284-1.
- [8] LIPKA, R.: Analytické pravdepodobnostní modely. Marsovské procesy, 2015 [online].
- [9] OSADSKÁ, V.: Stochastics methods in risk analysis. In: Safety Engineering Series, Vol. XII, 2017, No. 1, pp. 61-67.
- [10] RAUSAND, M. – HOYLAND, A.: System Reliability Theory, Models, Statistical Methods and Application. Second Edition. New Jersey, John Wiley and sons, 2004, 636 pages. ISBN 0-471-47133-X.
- [11] REDMILL, F. – ANDERSON T. (edit.): Developments in Risk-based Approaches to Safety: Proceedings of the Fourteenth Safety-critical Systems Symposium, Bristol, UK, Springer Science & Business Media, 2007. 292 pages. ISBN 10:1-846 28-333-7.
- [12] STANLEIGHT, M.: Business Improvements Achievements. Canada, Toronto, Ontario, ASQ, 2000 [online].
- [13] SHUMWAY, R. – STOFFER, D.: Time Series Analysis and Its Applications. Third Edition. New York: Springer, 2006. ISBN 978-1-4419-7864-6.
- [14] VAN DER NEUTA, R.: Uncertainty analysis in Bayesian Networks. Utrecht: Utrecht University, 2014. 119 pages [online].

PROFESIJNÝ ŽIVOTOPIS

Ing. Marek Hargaš absolvoval štúdium na Národohospodárskej fakulte Ekonomickej univerzity v Bratislave, odbor financie, bankovníctvo, investovanie. V rokoch 2003 – 2017 pôsobil vo viacerých súkromných podnikoch ako riaditeľ alebo podpredseda predstavenstva. Od roku 2017 je generálnym tajomníkom služobného úradu Štatistického úradu Slovenskej republiky.

KONTAKT

marek.hargas@statistics.sk