TESTOVANIE BEZPEČNOSTI OBJEKTOV VOČI VZDUŠNÉMU NARUŠITEĽOVI POMOCOU STROMU PORÚCH

Tomáš Kurpaš [*)] **Jaroslav Sivák** [**)]

ABSTRAKT

V našej práci sa venujeme problematike ochrany objektov kritickej infraštruktúry pred preniknutím narušiteľa do chráneného priestoru vzdušnou cestou. Cieľom práce je prostredníctvom výskumných metód a modelov identifikovať a definovať kritické faktory, ovplyvňujúce riešenie ochrany kritickej infraštruktúry pred vzdušným nevojenským ohrozením. Práve na nájdenie kritických faktorov sme na základe metódy analýzy stromu porúch vytvorili model, ktorý nám umožňuje identifikovať najslabšie články systému ochrany objektov pred jednotlivými kategóriami vzdušného narušiteľa. Uvedený model umožňuje otestovať navrhnuté, poprípade prijaté bezpečnostné opatrenia a jednoznačne určí oblasti, v ktorých je potrebná zvýšená pozornosť pri návrhu a realizácii ochrany prvku kritickej infraštruktúry.

Kľúčové slová: kritická infraštruktúra, model, analýza stromu porúch, vzdušné narušenie.

ABSTRACT

In our work, we are interested in critical infrastructure protection against the air intrusion into security area. Our aim is to find and define critical factors connected with security problems by aplication of research methods and models. To find critical factors, we created model based on Fault Tree Analysis, which is able to identify the weakest elements of security system to prevent aerial intrusion. This model alowes us to test designed or applied security measures and clearly determine areas, where the increased attention in the design and implementation of protection of critical infrastructure elements is necessary.

[*)] Tomáš, Kurpaš, Ing., Veliteľstvo vzdušných síl OS SR, Jána Jiskru 10, 96001 Zvolen, kurpast@gmail.com,
[**)] Jaroslav, Sivák, doc. Ing., CSc., MBA, QUADRIQ, a.s., Priemyselná 1, 03101 Liptovský Mikuláš, **jaroslav.sivak@quariq.sk**.

Key words: critical infrastructure, model, Fault Tree Analysis, aerial intrusion.

1 ÚVOD

Pri riešení problematiky ochrany objektov kritickej infraštruktúry (ďalej len KI) je našou úlohou identifikovať kritické faktory, vplývajúce na riešenie ich ochrany pred ohrozením zo vzduchu. Pod týmto ohrozením nie je myslený len priamy ničivý útok, ale hlavne prienik do chráneného perimetra vzdušnou cestou. Ako je uvedené nižšie, na vytvorenie modelu vhodného pre riešenie našej úlohy sme sa rozhodli použiť analytickú metódu analýzy stromu porúch (ďalej len FTA). Metóda svojim grafickým a jasným popisom jednotlivých vzťahov umožňuje vytvoriť všeobecný model na testovanie a nájdenie kritických ciest a konkrétnych kritických prvkov systému náchylných na zlyhanie. Nájdenie kritických faktorov nám poskytne základ, pre prijatie odporúčaní, poprípade pre ďalšie skúmanie týchto faktorov, aby sme dokázali zabezpečiť skutočne efektívnu ochranu prvku KI pred narušením zo vzduchu.

Model sme sa snažili zostaviť čo najjednoduchší a najpochopiteľnejší, aby bol schopný jednoduchým a pritom efektívnym spôsobom poskytnúť relevantné informácie o tom, či prijaté ochranné opatrenia testovaného objektu sú efektívne voči prípadnému narušeniu bezpečnosti zo vzduchu.

2 METÓDA ANALÝZY STROMU PORÚCH (FTA)

Metódu analýzy stromu poruchových stavov vyvinul v roku 1961 H. Watson z Bell Labs v spolupráci s A Mearnsom. Metóda bola vyvinutá pre potreby Vzdušných síl USA ako nástroj na hodnotenie povelového štartovacieho systému programu (rakety) Minuteman. Neskôr túto analytickú metódu prebrala firma Boeing, keď jej zamestnanec David Haasl zistil, že je účinným nástrojom pre analýzu bezpečnosti systému. Prvé masívne využitie našla uvedená metóda v rokoch 1964-67 a 1968-1999, kedy ju firma Boeing používala na bezpečnostné hodnotenie systémov programu Minuteman. Metóda analýzy stromu porúch sa postupne začala zavádzať vo vesmírnom priemysle (letectvo a zbrane) a v rokoch 1970 až 1980 bola úspešne zavedená aj jadrovom priemysle. Jej masívnejšie používanie podporilo vznik a rozširovanie softvérových nástrojov a kódov. V 80-tych rokoch minulého storočia prenikla metóda aj za hranice USA a vďaka jadrovému priemyslu sa začala používať medzinárodne [2].

Táto metodika je jedna z klasických metód na identifikáciu nebezpečenstva, ktorá sa zaraďuje medzi deduktívne metódy a svojou povahou ju možno zaradiť medzi špeciálne orientované grafy. Strom porúch má podobu logického diagramu a postupuje systematicky od symptómov - príznakov problému k ich príčinám, čím poskytuje prehľadný obraz o príčinách porúch na rôznych úrovniach. Môže kombinovať jednak rôzne poruchy strojov a technológií, ale i ľudské chyby. Metóda sa môže použiť tak na kvalitatívnu, ako aj kvantitatívnu analýzu, umožňuje pomerne jednoduché vyhľadanie „slabých miest“ systému a odhalí aspekty dôležité z hľadiska spoľahlivosti. Metóda je zameraná na konkrétnu nechcenú udalosť a poskytuje nástroj pre stanovenie príčin tejto udalosti. Nechcená udalosť prestavuje tzv. „top event“, čiže vrcholovú udalosť

v stromovom diagrame zostrojenom pre daný systém a všeobecne pozostáva z kompletného alebo katastrofického zlyhania systému.

Ako už bolo spomenuté skôr, táto metóda je sama o sebe grafickým modelom rôznych paralelných a sekvenčných kombinácií chýb, ktoré vyústia do preddefinovanej vrcholovej udalosti. Je potrebné si uvedomiť, že strom porúch nie je model všetkých možných chýb/zlyhaní systému, alebo všetkých možných príčin pre zlyhanie systému. Je prispôsobený jeho vrcholovej udalosti, ktorá korešponduje s niektorými konkrétnymi chybovými módmi systému a strom porúch obsahuje iba chyby, ktoré prispievajú k vzniku vrcholovej udalosti [5].

3 NÁVRH MODELU POMOCOU STROMU PORÚCH (FTA)

Pri riešení nášho problému, ktorým je nájdenie kritických faktorov ochrany objektu kritickej infraštruktúry pred vzdušným napadnutím, nebudeme využívať všetky možnosti, ktoré metóda analýzy stromu porúch poskytuje. Uvedená metóda nám však po zostavení stromu porúch umožní na základe vstupných údajov nájsť tzv. kritické cesty a určiť ich váhu, alebo prioritu.

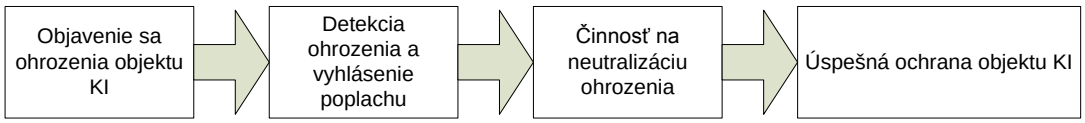
Proces zabezpečenia ochrany objektu je možné rozdeliť do dvoch základných častí a to detekcia, čiže zistenie približujúcej sa hrozby, narušiteľa, a následného vyhlásenia poplachu. Druhou časťou je vykonanie zásahu proti narušiteľovi. Zlyhanie činností jednej alebo druhej skupiny vedie k zlyhaniu celej ochrany objektu. To znamená, že narušiteľ či už nebol zistený, alebo zastavený ochrannými prostriedkami a činnosťou zásahovej jednotky, prenikol do chránenej zóny objektu. Práve takúto udalosť v našej práci považujeme za vrcholnú udalosť zlyhania systému.

V prípade použitia leteckých prostriedkov na prienik do chráneného priestoru je to pre narušiteľa jednoduchšie, lebo týmto spôsobom prekoná ochranné opatrenia, ako dotykové a tlakové senzory rozmiestnené v oblasti perimetra. Taktiež prekoná technické ochranné prostriedky fyzickej ochrany, akými sú ploty, valy, priekopy alebo ochranné steny. Zlyhanie detekcie takéhoto ohrozenia tiež vedie k tomu, že nie je možné vyhlásiť poplach a vykonať zákrok na zastavenie prieniku narušiteľa, keďže sa o ňom nevie.

Z pohľadu tvorby stromu porúch je dôležité zhodnotiť, či vznik vrcholovej udalosti zapríčiní zlyhanie detekcie, zlyhanie zásahu zásahovej jednotky, alebo je vznik vrcholovej udalosti podmienený len zlyhaním oboch činností naraz. Ak nie je narušiteľ detegovaný, nevieme o hrozbe, nevykoná sa žiaden zásah, narušiteľ prenikne a splní svoju úlohu. Ak je narušiteľ detegovaný, je vyhlásený poplach, ale z nejakého dôvodu sa ho nepodarí neutralizovať, narušiteľ prenikne. A keďže nemôže nastať situácia, že zásahová jednotka vykoná zásah bez toho aby bola úspešná detekcia narušiteľa, z toho vyplýva, že aby vznikla vrcholová udalosť, musia zlyhať obe vyššie popísané činnosti.

Pri návrhu modelu sme vychádzali z poznatkov ohľadom štandardného komplexu organizačných a technických opatrení pre zabezpečenie ochrany objektov, kde okrem legislatívnych nástrojov sú použité aj elektronické, alebo mechanické prostriedky na odradenie, detekciu a signalizáciu konania narušiteľa v chránenom priestore [3], [4]. Vytvorený model musí byť dostatočne konkrétny, ale nie až do takej miery, aby

sa nedal použiť aj na testovanie ochrany iného objektu KI. Istá úroveň všeobecnosti je potrebná, z toho dôvodu bude model zameraný na činnosti, ako v oblasti detekcie, tak aj zásahu. Model netestuje jednotlivé technické prvky ako napríklad kamerový systém či pohybové senzory. V časti modelu, ktorý sa bude zaoberať detekciou, testujeme a hodnotíme činnosti detekcie. Tento prístup nám umožní použiť vytvorený model na rôzne prvky kritickej infraštruktúry, ktoré používajú rôzne technické zariadenia pre zistenie narušiteľa. Okrem toho, že nám to umožňuje istú univerzálnosť modelu, pomôže nám to aj pri hľadaní kritických faktorov pre jednotlivé druhy vzdušných ohrození. Ako je známe, každý typ alebo kategória vzdušných prostriedkov má isté charakteristiky, ktoré ovplyvňujú parametre detektorov. Z toho vyplýva, že model, ktorý počas testovania využíva ako detektor napríklad kamerový systém, bude produkovať pre jednotlivé kategórie vzdušných prostriedkov iné kritické faktory, ktoré môžu viesť k vzniku vrcholovej udalosti. To isté platí aj v prípade činností vykonávaných pri zásahu. Jednotlivé prvky kritickej infraštruktúry môžu mať rôzne postupy zásahu, komunikácie, prípadne rôzne technické vybavenie. Táto diverzita sa prejaví pri testovaní systému proti konkrétnej kategórii vzdušných prostriedkov.



Obrázok 1 Model

Vytvorený model teda všeobecne otestuje, ohodnotí a nájde kritické faktory, ktoré majú zásadný vplyv na zabezpečenie ochrany prvku kritickej infraštruktúry pred prienikom zo vzduchu. Jeho adaptabilnosť na zmenu objektu či kategórie vzdušných prostriedkov je vykonávaná prostredníctvom zmeny vstupných údajov testovaných parametrov. Vstupné údaje jednotlivých parametrov v testovanom modeli vyjadrujú závislosť medzi použitými technickými prostriedkami, zásahovými činnosťami a kategóriami leteckých prostriedkov, ktoré môžu predstavovať hrozbu pre daný objekt. Táto závislosť bude vyjadrená pravdepodobnosťou nastania javu, ktorý je nebezpečný pre zlyhanie systému.

4 POPIS NAVRHNUTÉHO MODELU POMOCOU FTA

Model, ktorý sme zostavili pre otestovanie efektívnosti prijatých opatrení na ochranu objektu netestuje len mechanické a elektronické bezpečnostné opatrenia, ale aj organizačnú časť riešenia ochrany prvku kritickej infraštruktúry. Tieto dve základné časti alebo zložky opatrení na ochranu, popisujú dve základné činnosti a to zistenie, čiže detekciu narušiteľa a neutralizáciu, zásah proti narušiteľovi. Tak ako v oblasti detekcie, tak aj v oblasti neutralizácie narušiteľa sa navzájom prelínajú organizačné opatrenia s použitím mechanických, elektronických a zbraňových systémov. Model netestuje konkrétne organizačné opatrenia a konkrétne technické prostriedky. Nebolo by to efektívne a model by bolo možné použiť len na jeden konkrétny objekt. Rozhodli sme sa preto spraviť ho univerzálnejším a to nahradením konkrétnych testo-

vaných systémov a opatrení, činnosťami prebiehajúcimi v oboch spomenutých častiach – detekcii a neutralizácii. Použité činnosti sú vo väčšine prípadov totožné alebo obdobné, preto je možné model aplikovať na ľubovoľný prvok kritickej infraštruktúry.

Počas vytvárania modelu pomocou metódy FTA sme najprv museli rozobrať jednotlivé činnosti, ktoré sú vykonávané na zabezpečenie ochrany objektu. Po podrobnom rozobratí jednotlivých činností, ktoré sme sa snažili skúmať do čo najväčšej hĺbky, avšak len po istú hranicu, aby testovanie nebolo príliš komplikované a časovo náročné, sme si ich museli znegovať a pozrieť sa na ne z opačnej strany. To znamená, že sme skúmali, čo ovplyvní danú činnosť tak, aby bola neúspešná a aký ďalší vplyv to bude mať na zabezpečenie ochrany.

Postupom z vyšších úrovní činností k primárnym udalostiam sme hľadali práve tie prvotné udalosti, ktoré spôsobia zlyhanie činností na vyššej úrovni stromu. Tým sme našli „všetky" príčiny zlyhania detekcie a neutralizácie. Nájdenie týchto základných a nerozvinutých primárnych udalostí môžeme pokladať za nájdenie hľadaných faktorov, ktoré ovplyvňujú úspešnosť ochrany objektu KI. Navrhnutý model teda umožňuje stanoviť váhu jednotlivých faktorov, ktoré majú vplyv ma efektívnosť prijatých ochranných opatrení prvku KI proti konkrétnemu typu leteckých prostriedkov. Spomenuté určenie váh (dôležitosti) faktorov nám pomôže identifikovať najslabšie miesta v procese ochrany testovaného objektu a následne prijať adekvátne opatrenia na zlepšenie jeho ochrany a obrany.

Veľmi dôležitým faktom našej práce je, že nami použitá metóda stromu porúch je prioritne určená na testovanie spoľahlivosti a odolnosti systémov, hlavne technických systémov. My sme však skúmali jednotlivé činnosti a udalosti, ktoré by mohli viesť k ich zlyhaniu. Práve z tohto dôvodu sme museli metódu stromu porúch prispôsobiť na naše podmienky a naše úlohy.

Pri testovaní a hľadaní najslabších komponentov technického systému sa pri ich kvalitatívnej a kvantitatívnej analýze využívajú údaje ako stredná doba bezporuchovej činnosti a pod. čiže ide o údaje, ktoré jasne popisujú spoľahlivosť komponentov a sú poskytované či už výrobcom komponentu alebo štatistickými údajmi z rôznych databáz. Pri skúmaní našich faktorov sme takéto údaje vo väčšine prípadov nemali, lebo sa nejednalo o skúmanie spoľahlivosti komponentu systému, ale o činnosť, udalosť či faktor, ktorý má vplyv na činnosť na vyššej úrovni. Nemohli sme využívať štatistické údaje z rôznych databáz alebo do výrobcov, a preto sme si museli stanoviť určenie koeficientov dôležitosti sami. Koeficienty dôležitosti sme si stanovili najjednoduchšou dostupnou metódou a to stanovením si určitej stupnice a výberom hodnoty zo stupnice, ktorá by čo najvernejšie mohla popisovať dôležitosť skúmaného faktora v celom procese popísanom stromom porúch. Pre výpočet pravdepodobnosti nastania alebo objavenia sa danej udalosti (faktora) sme potom vychádzali z klasickej definície pravdepodobnosti.

5 ZÁVER

Pri návrhu modelu na testovanie ochrany objektu kritickej infraštruktúry pred vzdušným narušiteľom sme narazili na oblasti, ktorým je potrebné venovať zvýšenú pozornosť. Tieto zistenia nám ponúkajú jasné odpovede na to, čo je potrebné zlepšiť

pre zabezpečenie adekvátnej ochrany voči zneužitiu leteckých prostriedkov ako formy ohrozenia objektu. Navrhnutý model stromu porúch, ktorý je možné použiť na rôzne prvky KI sme overili na príklade pomocou softvérových nástrojov, určených na vykonanie analýzy FTA. Je však potrebné si uvedomiť jednu dôležitú vec a to, že navrhnutý model nie je „uzamknutý“ a je ho možné v prípade potreby rozšíriť o niektoré špecifické činnosti, aby dokázal skutočne čo najdôveryhodnejšie popísať stav a efektívnosť prijatých opatrení voči vzdušnému narušeniu.

Výsledkom našej práce je zistenie, že metóda FTA, ktorá je prioritne určená na testovanie spoľahlivosti technických systémov, je možné celkom efektívne použiť aj pri testovaní bezpečnostných opatrení prvkov kritickej infraštruktúry, v našom prípade proti ohrozeniam zo vzduchu.

LITERATÚRA

[1] KUBEK, J.: Štýl článku. FŠI ŽU. Žilina: Vydavateľstvo ŽU 2001. 23 s. In.:

[2] VESELY, W.E., GOLDBERG, F.F.: Fault Tree Handbook. U.S. Nuclear Regulatory Commission. Washington, D.C.: Office of Nuclear Regulatory Research 1981.

[3] Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany. [online]. Bratislava, 2006. [cit. 2010-07-21]. Dostupné na: **http://www.minv.sk/?ochrana-kritickej-infrastruktury**

[4] Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike. Vláda Slovenskej republiky, . [online]. Bratislava, 2007. [cit. 2010-07-21]. Dostupné na: **http://www.minv.sk/?ochrana-kritickej-infrastruktury**

[5] **http://fsi.utc.sk/kkm/publikacie/kp/kp_kap_8.pdf**

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