ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA BEZPEČNOSTNÉHO INŽINIERSTVA
KRÍZOVÝ MANAŽMENT - 2/2018
ISSN:1336 - 0019
str. 51 - 59

ODOLNOSŤ PRVKOV KRITICKEJ INFRAŠTRUKTÚRY

RESILIENCE OF CRITICAL INFRASTRUCTURE ELEMENTS

Nikola CHOVANČÍKOVÁ[1]

ABSTRACT:

Infrastructure is a key component of each country's sustainable development. All countries need efficient transport, energetic and communication systems which are indispensable for maintaining of the population´s living standard and for the functioning of the individual state´s components. These components also include those which when destructed or damaged would have a serious impact on the functioning of the state. In the state system such parts are referred to as critical infrastructure. Therefore, international organizations as well as individual states, are striving to achieve the required level of security for these key components. When increasing security levels, object operators should be also interested in resilience that has a significant impact on both the safety and the functioning of the element. Which features will work if the critical infrastructure element is damaged depends from the degree of resilience.

KEYWORDS: *critical infrastructure, level of safety, resilience.*

ÚVOD

„Kritická infraštruktúra (ďalej len KI) má v rámci bezpečnostnej politiky štátu zásadný význam. Každý jej prvok môže ohroziť bezpečnosť, ekonomické záujmy či samotný chod štátu a zasiahnuť do každodenného života spoločnosti [13].“

Škody na kritickej infraštruktúre, jej zničenie alebo narušenie prírodnými katastrofami, terorizmom, kriminálnou činnosťou alebo inými negatívnymi faktormi, môžu mať negatívny vplyv nie len na samotný štát ale i na susedské štáty. Preto je potrebné sa touto problematikou aktívne zaoberať a neustále zlepšovať ochranu prvkov kritickej infraštruktúry. Pre zaistenie požadovanej úrovne bezpečnosti prvkov kritickej infraštruktúry je potrebné sa sústrediť na ich odolnosť. Práve odolnosť determinuje, ktoré funkcie si je schopný prvok zachovať pri negatívnom pôsobení nežiaducich javov. Aby boli zachované základné funkcie prvku musí mať určitú úroveň odolnosti. Vysoká úroveň odolnosti prvku umožní pri jeho narušení zachovanie nevyhnutných funkcií pre zaistenie fungovania prvku.

1. ODOLNOSŤ PRVKOV KRITICKEJ INFRAŠTRUKTÚRY

Problematika odolnosti prvkov kritickej infraštruktúry na území Slovenskej republiky ešte nebola riešená. Odolnosti kritickej infraštruktúry sa doposiaľ venovali len na akademickej pôde Fakulty bezpečnostného inžinierstva pri projekte „Metodika hodnotenia resiliencie prvkov kritickej infraštruktúry“ v spolupráci s Technickou univerzitou v Ostrave. Táto metodika bola spracovaná za podpory grantového projektu VI20152019049 „Resilience 2015: Dynamické hodnotenie odolnosti súvzťažných subsystémov kritickej infraštruktúry“ podporeného Ministerstvom vnútra Českej republiky v rokoch 2015-2019. Na pôde fakulty bol tiež spracovaný projekt APVV-0471-10, ktorý sa zameriaval na ochranu kritickej infraštruktúry v sektore doprava.

V súčasnosti je vhodné sa zaoberať problematikou odolnosti, keďže sa nachádzame v dobe, kedy sa často vyskytujú mimoriadne udalosti, ktoré ohrozujú život obyvateľov i fungovanie štátu. Je veľmi dôležité, aby sa zabezpečilo kvalitné vybavenie a pripravenie potenciálnych prvkov kritickej infraštruktúry tak, aby dokázali odolať a rýchlo obnoviť základné funkcie.

[1] Nikola Chovančíková, Ing., Fakulta bezpečnostného inžinierstva Žilinskej univerzity v Žiline, Univerzitná 8125/1, 010 26 Žilina, Slovenská republika, tel.: +421 41 513 6668, e-mail: nikola.chovancikova@fbi.uniza.sk.

Pre zabezpečenie požadovanej úrovne bezpečnosti je potrebné sa zamerať na odolnosť prvku. Práve odolnosť zodpovedá za to, ktoré funkcie si je schopný prvok zachovať pri narušení.

Odolnosť (resilience) je vnímaná ako schopnosť systému absorbovať narušenie, znášať negatívne zmeny systému, a pritom zabezpečiť kľúčové funkcie, štruktúru a spätnú väzbu systému. Predstavuje vnútornú pripravenosť subsystémov kritickej infraštruktúry odolávať nežiaducim udalostiam, poprípade schopnosť subsystémov zaistiť a udržať si svoje funkcie pri negatívnym pôsobení vonkajších alebo vnútorných faktorov [3].

Stanovenie odolnosti je z pohľadu ochrany kritickej infraštruktúry veľmi dôležité.

Odolnosť kritickej infraštruktúry alebo jej prvku vyjadruje vzájomné pôsobenie negatívnych faktorov z interného alebo externého prostredia. Podstatným krokom pri stanovení miery odolnosti je formulácia jej ukazovateľov. Medzi tieto ukazovatele patria nasledujúce:

Robustnosť (redundancy) – je určená ako vnútorná odolnosť systému voči externým faktorom. Spadajú sem technické a organizačné aspekty v rámci, ktorých ide predovšetkým o dodržiavanie konštrukčných noriem, využívanie technologických postupov i využívanie krízového a núdzového plánovania. Podstatnou časťou robustnosti sú bezpečnostné opatrenia prvku medzi, ktoré patrí fyzická ochrana, technologické zariadenia a systémy.

Redundancia (robustness) – je chápaná ako schopnosť systému využívať alternatívne voľby a zdroje v procese riešenia porúch a bezpečnostných incidentov.

Reakcieschopnosť (responsiveness) – pre prvok kritickej infraštruktúry spočíva v schopnosti mobilizovať a využívať všetky dostupné zdroje a prostriedky v prípade mimoriadnej udalosti. Predpokladom účinnej reakscieschopnosti je dostupnosť zdrojov a materiálov pre záchranné a likvidačné práce [1].

Odolnosť patrí k významným faktorom procesu manažérstva ochrany prvku kritickej infraštruktúry. Proces manažérstva ochrany prvku kritickej infraštruktúry môžeme vidieť na obrázku 1.

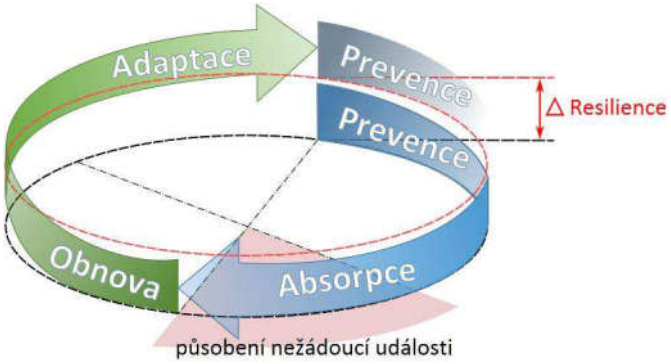
Obrázok 1 **Proces manažérstva ochrany prvku kritickej infraštruktúry** [4]

Určovanie prvkov kritickej infraštruktúry je prvým subprocesom manažérstva ochrany. Základ tohto procesu je určenie častí verejných a súkromných infraštruktúr, ktoré podľa Smernice rady 2008/114/ES o európskych kritických infraštruktúrach, spĺňajú sektorové alebo prierezové kritéria európskej kritickej infraštruktúry alebo spĺňajú podmienky prvku národnej KI, podľa zákona č. 45/2011 o kritickej infraštruktúre.

Druhým krokom v rámci procesu manažérstva ochrany je posudzovanie prvku kritickej infraštruktúry. Posudzovanie spočíva vo vyhodnotení rizík v posúdených relevantných scenárov nežiaducich udalostí a vyhodnotenie odolnosti (technickej, organizačnej) záujmového prvku v posúdení jeho robustnosti, obnoviteľnosti a adaptability [4].

Poslednou časťou procesu manažérstva ochrany je zabezpečenie ochrany prvkov kritickej infraštruktúry, ktorá spočíva v zvládaní rizík a posilňovaniu odolnosti vhodnými prostriedkami. Zvládanie rizík zahrňuje výber a implementáciu jedného alebo viacerých variantov na elimináciu rizík. Posilňovaním odolnosti dochádza k minimalizácií zraniteľnosti subsystémov [4].

Zvládanie rizík i posilňovanie odolnosti prispieva k minimalizácií rizík, ktoré by mohli narušiť fungovanie prvku kritickej infraštruktúry. Posilňovanie spoločne s hodnotením odolnosti tvoria základ pre jej pochopenie. Odolnosť v systéme kritickej infraštruktúry predstavuje cyklický proces a jeho podstatou je permanentné zlepšovanie prevencie, absorpcie, obnovy a adaptácie systému [4].



Obrázok 2 **Cyklus odolnosti kritickej infraštruktúry** [4].
(Zdroj: Metodika hodnocení resilience prvků kritické infrastruktury. 2018, s. 8)

Prevencia je prvou fázou cyklu odolnosti. Realizácia preventívnych opatrení je podľa zákona č. 45/2011 o ochrane kritickej infraštruktúry v rukách prevádzkovateľa prvku KI, ktorého povinnosti sú vymedzené v zákone. Aplikáciou opatrení sa pripravuje systém na nežiadúce udalosti, ktoré by mohli nastať v budúcnosti. V prípade pôsobenia negatívnych udalostí systém prechádza do fázy absorpcie. Absorpcia je podnietená vplyvom pôsobenia negatívnych udalostí, a je determinovaná robustnosťou subsystému KI. Ako bolo spomenuté na začiatku kapitoly, robustnosť je schopnosť systému odolávať pôsobeniu nežiaducich udalostí bez toho, aby došlo k výpadku služieb, ktoré objekt poskytuje.

Po skončení pôsobenia nežiaducej udalosti prechádza systém do fázy obnovy. Táto fáza sa vyznačuje obnoviteľnosťou, to znamená schopnosťou systému obnoviť svoju činnosť do požadovanej úrovne. Obnova je vymedzená dostupnosťou zdrojov a časom, ktorý je nutný na realizáciu obnovy procesov [4].

Poslednú fázu odolnosti predstavuje adaptácia. Ide o schopnosť organizácie adaptovať prevádzkovaný systém na prípadné opakovanie nežiaducej udalosti. Adaptácia je vymedzená vnútornými procesmi organizácie, ktoré smerujú k posilňovaniu odolnosti, ako je napríklad manažérstvo rizík alebo vzdelávací proces. Zvyšovaniu odolnosti systému môže dochádzať už vo fáze obnovy, napríklad formou výmeny komponentov [4].

2. HODNOTENIE ODOLNOSTI

Hodnotenie odolnosti bolo rozoberané v rámci diplomovej práce Metodika hodnotenia odolnosti vybraných prvkov a systémov prvkov kritickej infraštruktúry, ktorá bola podporovaná projektom Systém hodnotenia odolnosti prvkov a sietí vybraných oblastí KI na území ČR. Momentálne sa hodnoteniu odolnosti venuje projekt CIERA (Critical Infrastructure Elements Resilience Assessment), ktorý bol spomenutý v prvej kapitole. Výpočet odolnosti bol smerovaný do oblasti elektorenergetiky. Tento podsektor kritickej infraštruktúry je v súčasnosti veľmi dôležitým, keďže elektrická energia je neoddeliteľnou súčasťou ľudskej existencie. „Slúži na zabezpečenie základných životných potrieb obyvateľstva, zdravia obyvateľstva a má významný vplyv aj na ekonomiku a bezpečnosť štátu [14].“Postup vyčíslenia odolnosti potenciálneho prvku kritickej infraštruktúry z oblasti elektroenergetiky bol prevzatý z Metodiky hodnotenia odolnosti vybraných prvkov a systémov prvkov KI, ktorý stanovuje postup riešenia nasledovne:

a) systémová analýza hodnoteného prvku KI,

Systémová analýza predstavuje úvodnú fázu hodnotenie odolnosti prvku KI. Zameriava sa na zoznámenie sa s detailmi prvku, a to: cieľová funkcia prvku, kľúčové procesy, počet zamestnancov a iné. Výstupným dokumentom systémovej analýzy je globálna architektúra prvku. Globálna architektúra prvku je dokument, ktorý obsahuje prehľad kľúčových

procesov, technológií používaných k zaisteniu kľúčových procesov a ochrany prvku kritickej infraštruktúry, systémových prvkov topologicky usporiadaných [5].

b) analýza a hodnotenie rizík,

Analýza predstavuje nevyhnutný nástroj pre odhalenie rizík. Pomáha identifikovať a pochopiť riziká, ktorými by mohol byť potenciálny prvok kritickej infraštruktúry ohrozený. Prvým krokom v rámci analýzy je identifikácia možných hrozieb pre prvok KI a následný odhad pravdepodobnosti ich vzniku [5]. Proces analýzy rizík bude dvojstupňový vzhľadom k potrebe komplexného prístupu k hodnoteniu a analýze rizík. Súčasťou procesu analýzy a hodnotenia rizík sú:

- prvotná semi-kvantitatívna analýza rizík,
- KARS analýza.

c) stanovenie hodnotených oblastí bezpečnosti,

Špecifikácia a determinovanie oblasti bezpečnosti je základnou fázou procesu hodnotenia odolnosti. Súbor identifikovaných rizík a ich následná redukcia, poprípade eliminácia si vyžaduje určenie konkrétnych oblastí bezpečnosti. Pre ďalší proces hodnotenia odolnosti boli na základe aktuálneho stavu stanovené tieto oblasti bezpečnosti:

- fyzická bezpečnosť,
- informačná bezpečnosť,
- administratívna bezpečnosť,
- personálna bezpečnosť,
- bezpečnosť a ochrana zdravia pri práci,
- a iné.

d) určenie hodnôt atribútov a výpočet veľkosti ukazovateľov,

V rámci tejto etapy hodnotenia budú identifikované všetky parametre (premenné) potrebné k vlastnému hodnoteniu a výpočtu ukazovateľov odolnosti. Parametre budú odrážať kvalitatívnu a kvantitatívnu stránku vymedzených oblastí zabezpečenia. Formálnym nástrojom pre zaistenie jednotlivých parametrov budú check listy. Využitie check listov umožní získať potrebné údaje pre stanovenie veľkosti ukazovateľov [5]. Jedná sa o nasledujúce ukazovatele a parametre:

H_{RZ} Koeficient rizikovosti

Interpretuje potenciálny dopad rizika na funkčnosť kritickej infraštruktúry. Vzťah (1-H_{RZi}) nám vyjadruje skutočnosť, že hodnota rizikovosti nám negatívnym spôsobom ovplyvňuje hodnotu odolnosti. Pri stanovení hodnoty poprípade parametru/koeficientu H_{RZi} sa vyberú riziká, ktoré je možné považovať za kritické (nachádzajú sa v I. kvadrante KARS analýzy – primárne a sekundárne nebezpečné riziká). Týmto rizikám sa pridelí hodnota z bodovej metódy. V prípade, že by hodnoty neboli v rozsahu <0,1> využije sa nasledovný vzťah:

$$H_{RZi} = \frac{H_{Ri}}{H_{Rimax}} \quad (1)$$

Kde:

H_{RZi} – je hodnota rizikovosti i-tého rizika v rozsahu <0,1>,

H_{Ri} – hodnota rizika vyplývajúca z prvej analýzy tzn. z bodovej metódy,

H_{RZi} – je maximálne dosiahnuteľná hodnota rizika v rámci hodnotovej škály [5].

H_{SO} Koeficient súvzťažnosti

Interpretuje závislosť a väzby medzi jednotlivými oblasťami a odvetviami kritickej infraštruktúry.

$$K_s = \frac{\sum S_i}{S_{max}} \quad (2)$$

Kde:

K_s – je koeficient súvzťažnosti,

$\sum S_i$ – je súčet miery závislosti i-tej skupiny prvkov na ostatné oblasti kritickej infraštruktúry,

S_{max} – maximálna hodnota, ktorú môžeme v rámci vymedzeného systému dosiahnuť [5].

K_{RO} Koeficient robustnosti

Interpretuje stav a úroveň bezpečnostných opatrení.

$$K_{RO} = K_{RZ} * K_{SR} \quad (3)$$

K_{RZ} – koeficient robustnosti zabezpečenia,

K_{SR} – koeficient štrukturálnej robustnosti [5].

K_{RZ} Koeficient robustnosti zabezpečenia

Koeficient robustnosti zabezpečenia vypočítame podľa nasledujúceho vzťahu:

$$K_{RZ} = M_{FB} * V_{FB} + M_{IB} * V_{IB} + M_{AB} * V_{AB} + M_{PB} * V_{PB} \quad (4)$$

Kde:

M_{FB} – je vyjadrenie miery kvality prijatých opatrení fyzickej bezpečnosti,

M_{IB} – je vyjadrenie miery kvality prijatých opatrení informačnej bezpečnosti,

M_{AB} – je vyjadrenie miery kvality prijatých opatrení administratívnej bezpečnosti,

M_{PB} – je vyjadrenie miery kvality prijatých opatrení personálnej bezpečnosti.

Vyjadrenie mier v jednotlivých oblastiach získame prostredníctvom vyplnenia checklistov. Po ich vyplnení je získaný prehľad o tom, ktoré opatrenia v jednotlivých oblastiach má podnik splnené.

V_{FB} – je váha fyzickej bezpečnosti,

V_{IB} – je váha informačnej bezpečnosti,

V_{AB} – je váha administratívnej bezpečnosti,

V_{PB} – je váha personálnej bezpečnosti [5].

Stanovenie váh jednotlivých oblastí robustnosti zabezpečenia je vykonané prostredníctvom metódy párového porovnania. Pri porovnávaní 2 kritérií poprípade variantov je významnejší variant hodnotený číslom „1“ a menej významný variant, t.j. horšie riešenie má hodnotu „0“. Ak by nastal prípad rovnakej dôležitosti variantov sa použije hodnota „1/2“ resp. „0,5“ [6].

Pre vyjadrení miery kvality prijatých opatrení v jednotlivých oblastiach robustnosti sú vyjadrené vzťahom:

$$M_i = \frac{\sum K_i}{x_i} \tag{5}$$

M_i – je vyjadrenie miery kvality prijatých opatrení v i-tej oblasti robustnosti,

$\sum K_i$ – je počet naplnených o kritérií,

x_i – je celkový počet stanovených kritérií v i-tej oblasti robustnosti.

K_{SR} Koeficient štrukturálnej robustnosti

$$K_{SR} = 0{,}8 + \frac{I_t + I_s + I_{kt} + I_f + I_r + I_{po}}{60} \tag{6}$$

K_{SR} – koeficient štrukturálnej robustnosti,

I_t – je index topológie,

I_s – je index zložitosti,

I_{kt} – je index kľúčových technológií,

I_f – je index flexibility,

I_r – je index redundancie,

I_{po} – je index perimetrickej ochrany.

K_{PR} koeficient pripravenosti

Interpretuje schopnosť prvku zaistiť odozvu na vznik mimoriadnej udalosti a obnovu požadovaných funkcií prvku kritickej infraštruktúry [5].

Matematické vyjadrenie pripravenosti vybraného prvku kritickej infraštruktúry je dané vzťahom:

$$K_{PR} = \frac{K_r + K_p + K_i}{3} \tag{7}$$

Kde:

K_r – je koeficient správnosti identifikovaných rizík,

K_p – je koeficient kvality spracovania bezpečnostného plánu,

K_i – je koeficient kvality implementácie bezpečnostného plánu.

Koeficient správnosti identifikácie rizík K_r, vyjadruje do akej miery sú v bezpečnostnom pláne správne identifikované riziká. Koeficient správnosti identifikácie je vyjadrený vzťahom:

$$K_r = \frac{R_p}{R_i} \tag{8}$$

R_p – vyjadruje koľko rizík zo zoznamu významných rizík identifikovaných hodnotiteľom je uvedených v bezpečnostnom pláne,

R_i – vyjadruje, koľko rizík bolo hodnotiteľom identifikovaných.

Ďalším krom je stanovenie koeficientu kvality spracovania plánu, ktorý je vydrený vzťahom:

$$K_p = \frac{\sum K_{ip}}{x_i} \tag{9}$$

K_{ii} – počet naplnených kritérií v rámci kontrolného zoznamu,

x_i – je celkový počet stanovených kritérií v danej oblasti pripravenosti.

e) výpočet stupňa odolnosti prvku KI

Multikriteriálne hodnotenie predstavuje najvhodnejšiu metódu pre hodnotenie odolnosti prvkov a systémov KI. Umožňuje realizovať ucelené hodnotenie relatívne nezávislých ukazovateľov a parametrov [5].

Pre komplexné multikriteriálne hodnotenie odolnosti vybraného prvku alebo systému KI bol stanovený matematický vzťah:

$$ODP = \frac{\sum OD_i}{x_i} \quad (10)$$

ODP – je hodnota odolnosti hodnoteného prvku KI,
OD_i – hodnota odolnosti prvku vo vzťahu k vybranému riziku,
x_i – je počet vybraných rizík

Matematické vyjadrenie hodnotenia odolnosti prvku kritickej infraštruktúry je vyjadrené vzťahom:

$$OD_i = \frac{(1-H_{RZi})+(1-K_S)+(K_{RO}*V_{RO}+K_{PR}*V_{PR})}{3} \quad (11)$$

R_{Zi} – je hodnota rizikovosti i-tého rizika,
K_S – je koeficient súvzťažnosti,
K_{RO} – je koeficient robustnosti,
K_{PR} – je koeficient pripravenosti,
V_{RO} – váha robustnosti,
V_{PR} – váha pripravenosti [5].

Tabuľka 1 **Vyhodnotenie odolnosti prvku KI - stupnica hodnotenia odolnosti** [5]

Hodnotenie	Hodnota	Slovné hodnotenie
Výborne (A)	0,8-1	Na všetky identifikované riziká je pripravený, žiadne z rizík nie je zanedbané vo fungovaní nedochádza k poruchám, kvalita a rozsah opatrení presahujú možné dopady a dôsledky ujmy
Veľmi dobre (B)	0,6-0,79	Na všetky dôležité identifikované riziká je pripravený, za určitých podmienok a ojedinele nie je obnova zaistená v norme
Dobre (C)	0,4-0,59	Na väčšinu dôležitých identifikovaných rizík je pripravený, obnova funkcie je zaistená vo väčšine prípadov v norme
Dostatočne (D)	0,2-0,39	Na väčšinu identifikovaných rizík je pripravený, je schopný obnovy funkcie ale vo väčšine prípadov doba obnovy presiahne štandard
Nie je schopný odolať (E)	0-0,19	Na väčšinu identifikovaných rizík nie je pripravený, nemá systém pre zaistenie obnovy funkcie

3. VYHODNOTENIE ODOLNOSTI PRVKU KI

Keďže výpočet odolnosti je veľmi zdĺhavý, v tejto časti bude zobrazený konečný výpočet odolnosti s následným stanovením stupňa odolnosti s možnými navrhovanými opatreniami, ak by bola odolnosť potenciálneho prvku nedostatočná.

Za hodnotený potenciálny prvok bola vybratá spoločnosť XY, a. s.

Prioritnou úlohou je distribúcia elektrickej energie do Žilinského, Banskobystrického a do časti Trenčianskeho kraja pre takmer 740 000 zákazníkov. Okrem distribúcie elektrickej energie sa spoločnosť venuje i montáži a oprave meracej a regulačnej techniky, poradenskej činnosti v energetike, projektovaniu a konštruovaniu elektrických zariadení, a iné [2].

Po dosadení a stanovení jednotlivých ukazovateľov, sme sa dopracovali až ku konečnému vzťahu, ktorý určí stupeň odolnosti hodnoteného potenciálneho prvku.

$$OD_i = \frac{(1-H_{RZi})+(1-K_S)+(K_{RO}*V_{RO}+K_{PR}*V_{PR})}{3}$$

Po dosadení hodnôt do matematického vzťahu sme získali nasledovné výsledky:

$$OD_1 = \frac{(1-0{,}6)+(1-0{,}61)+(0{,}75*0{,}5+0{,}68*0{,}5)}{3} = 0{,}501$$

$$OD_2 = \frac{(1-0{,}6)+(1-0{,}61)+(0{,}75*0{,}5+0{,}68*0{,}5)}{3} = 0{,}501$$

$$OD_3 = \frac{(1-0{,}64)+(1-0{,}61)+(0{,}75*0{,}5+0{,}68*0{,}5)}{3} = 0{,}491$$

$$OD_4 = \frac{(1-0{,}6)+(1-0{,}61)+(0{,}75*0{,}5+0{,}68*0{,}5)}{3} = 0{,}501$$

Vzhľadom k tomu, že celková hodnota odolnosti v rámci posudzovaného systému je priemernou hodnou odolnosti systému vo vzťahu k i-tému riziku, tak na základe vyjadrených hodnôt, je možné stanoviť celkovú odolnosť potenciálnemu prvku na základe vzťahu:

$$ODP = \frac{\sum OD_i}{x_i}$$

$$ODP = \frac{OD_1 + OD_2 + OD_3 + OD_4}{4}$$

$$ODP = \frac{0{,}501 + 0{,}501 + 0{,}501 + 0{,}491}{4}$$

$$ODP = 0{,}499$$

Po vyčíslení odolnosti prvku a jeho zaradenia podľa stupnice hodnotenia odolnosti, je možné konštatovať, že: prvok je hodnotený ako dobre zabezpečený „C“. Z toho vyplýva, že je na väčšinu dôležitých identifikovaných rizík pripravený, a v prípade narušenia je obnova funkcií vo väčšine prípadov zaistená v norme.

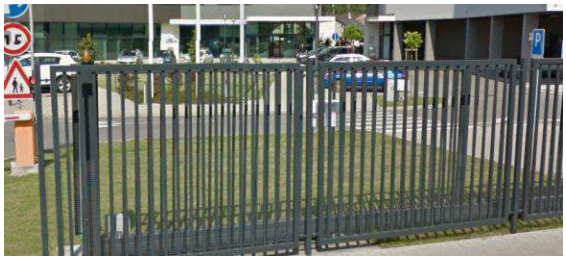
I keď je prvok dobre zabezpečený existujú malé nedostatky, ktoré by mohli byť odstránené navrhovanými opatreniami. Navrhované preventívne opatrenia môžu viesť k zvýšeniu stanovenej odolnosti a tým i zvýšeniu úrovne bezpečnosti potenciálneho prvku KI.

Preventívne opatrenia sú navrhované pre nasledovné oblasti zabezpečenia, a to:
- fyzická bezpečnosť,
- informačná bezpečnosť,
- administratívna bezpečnosť,
- personálna bezpečnosť.

Fyzická bezpečnosť

Fyzická bezpečnosť predstavuje systém opatrení aj na ochranu utajovaných skutočností, citlivých informácií pred nepovolenými osobami a pred neoprávnenou manipuláciou v objektoch a chránených priestoroch. Ochrana je zabezpečovaná prostredníctvom aplikácie mechanických zábranných prostriedkov, technických zabezpečovacích prostriedkov, fyzickou ochranou, režimovými opatrenia a ich vzájomnou kombináciu [7].

Pri navrhovaní opatrení fyzickej bezpečnosti sa vychádzalo z metodického usmernenia č. 290014/2014-1000-53190 Ministerstva hospodárstva Slovenskej republiky, v ktorom sú stručne popísané bezpečnostné opatrenia na ochranu prvkov kritickej infraštruktúry v sektoroch energetika a priemysel. Hranica areálu objektu je z prednej strany tvorená pevnou zváranou konštrukciou, pozri obrázok 3, ktorej súčasťou je brána na automatický pohon, ktorá umožňuje vjazd do objektu a výjazd z objektu.



Obrázok 3 **Oplotenie objektu z prednej časti**

Podľa usmernenia Ministerstva hospodárstva SR by malo byť oplotenie prednej strany objektu doplnené bavoletom a podhrabovými zábranami, obrázok 4.

Obrázok 4 **Plotové dielce i s nainštalovaným bavoletom** [12]

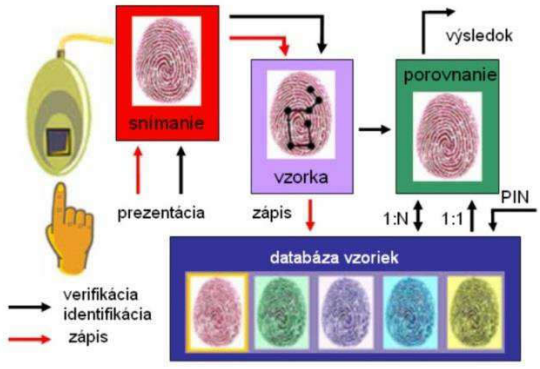
Informačná bezpečnosť

Informačná bezpečnosť je disciplína, ktorá spojuje poznatky a metódy z informatiky, softvérového inžinierstva, manažmentu, práva a iných vedných disciplín. Vystihuje ju multidisciplinárny charakter a veľmi rýchly rozvoj. Základným stavebným prvkom

v systéme sú dáta a informácie, ktoré je potreba chrániť, preto je dôležité charakterizovať požiadavky, ktoré kladieme na bezpečnostný systém a ako ich chceme zabezpečiť [8]. Preto by mali spoločnosti aplikovať nové právne predpisy, technológie a techniky, ktorými by si zaistili vysokú úroveň bezpečnosti informačných systémov.

Informačná bezpečnosť hodnotenej spoločnosti je na vysokej úrovni, ale súčasný pokrok v oblasti informatiky umožňuje neustále zvyšovanie úrovne využitím nových metód a techník.

Pre zlepšenie informačnej bezpečnosti by bolo odporúčané využitie biometrie v spoločnosti. Biometria je súbor metód určených na identifikáciu osôb podľa fyziologických znakov alebo zvykových znakov fyzickej osoby. Medzi fyziologické znaky môžeme zaradiť napríklad odtlačok prsta, obraz tváre, rozmery ruky a k zvykovým znakom patria podpis, hlas a iné. Pre mnou skúmaný potenciálny prvok kritickej infraštruktúry, by som navrhovala nainštalovať pred miestnosti, kde sa nachádzajú utajované dáta, zariadenia na snímanie odtlačkov prstov. Identifikácia prostredníctvom odtlačkov prstov je jednou z najznámejších a najviac publikovaných biometrických metód. Odtlačok prsta sa používa pre identifikáciu už celé storočia, a to hlavne kvôli svojej vlastnosti jedinečnosti a trvácnosti v čase.



Obrázok 5 **Postup identifikácie odtlačku prsta** [11]

Administratívna bezpečnosť

Administratívna bezpečnosť tvorí systém opatrení pri tvorbe, príjme, evidencií, spracovaní, odosielaní, preprave, prenášaní, ukladaní, skartovaní, archivácií, prípadne inej manipulácií s utajovanými informáciami. Na Slovensku je administratívna bezpečnosť upravená vyhláškou č. 453/2007 Z. z. vyhláška Národného bezpečnostného úradu o administratívnej bezpečnosti. Vyhláška pojednáva o manipulácií s utajovanými skutočnosťami, o ochrane utajovaných písomností poskytnutých a prijatých v rámci medzinárodnej spolupráce, o spoločných, prechodných a záverečných ustanoveniach.

Nasledujúce navrhované opatrenia by mali byť aplikované hlavne pri dokumentoch, ktoré sú podľa vyhlášky označované za tajné a prísne tajné. Ich ochrana by mala byť prioritou spoločnosti. Väčšia prostredí si vyžaduje, aby rôzne činnosti v rámci správy systému administratívnej bezpečnosti vykonávali odlišní užívatelia. Pri veľkých spoločnostiach sú rozdelené úlohy medzi viacerých pracovníkov a každý pracovník má v systéme rozličné postavenie i právomoci. Preto je dôležité, aby bol zavedený systém, ktorý presne definuje k čomu má daný pracovník prístup a aké úlohy môže vykonávať. V spoločnosti by malo byť zavedené **riadenie prístupu na základe rolí,** ktoré by zvýšil úroveň bezpečnosti. Riadenie prístupu na základe rolí funguje tak, že členom, t.j. zamestnancom, sú pridelené určité roly, a prostredníctvom týchto priradených rolí získavajú oprávnenia na vykonávanie konkrétnych činností v rámci počítačového systému [9].

Personálna bezpečnosť

Pri pojednávaní o personálnej bezpečnosti si treba uvedomiť, že práve ľudský element v informačnom systéme býva jeho najzraniteľnejším miestom. Ak sa k tomu pridá podceňovanie opatrení personálnej bezpečnosti a nedostatočné bezpečnostné povedomie zamestnancov, predstavuje to priam otvorené dvere do vnútra spoločnosti [10].

Na základe preštudovaných podkladov je možné tvrdiť, že spoločnosť má personálnu bezpečnosť dobre zabezpečenú, a preto v tejto oblasti nie sú uvedené žiadne preventívne opatrenia.

ZÁVER

Cieľom článku bolo poukázať na súčasné riešenie problematiky odolnosti prvkov kritickej infraštruktúry a priblíženie metodiky výpočtu odolnosti. Metodika bola aplikovaná na potenciálnom prvku kritickej infraštruktúry s cieľom zhodnotiť jeho odolnosť a navrhnúť

možné preventívne opatrenia, ktoré by mohli byť v praxi aplikované. Postup metodiky bol kvôli svojej rozsiahlosti skrátený len na konkrétne vyčíslenie odolnosti, ktoré tvorilo podstatnú časť, od ktorej sa odvíjali preventívne opatrenia pre prvok.

LITERATÚRA

[1] CHOVANČÍKOVÁ, N., 2016. *Prístupy a spôsoby k ochrane prvkov kritickej infraštruktúry v sektore Energetika v Českej republike*. Bakalárska práca. Žilina: FBI ŽU.

[2] *Výročná správa 2016* [online]. Stredoslovenská energetika- distribúcia. Dostupné z: https://www.ssd.sk/buxus/docs/dokumenty/o_nas/vyrocne_spravy/SSE%2017-037%20Vyrocna%20sprava%202016-DISTRIBUCIA-online.pdf

[3] HROMADA, M. 2010. *Stanovení odolnosti kritickej infraštruktúry – teoretický rámec/Critical Infrastructure Resilience Determination – Theoretical Framework*. In. Security Magazín. č. 93, str. 26-27. ISSN –1210-8723.

[4] ŘEHÁK, D. a kol. *Metodika hodnocení resilience prvků kritické infrastruktury.* Ostrava: VŠB – Technická univerzita Ostrava, 2018

[5] HROMADA, M. 2013. *Metodika hodnocení odolnosti vybraných prvků a systému prvků kritické infrastruktúry.* Diplomová práca. Univerzita Tomáše Bati v Zlíne.

[6] MÁCA, J., LEITNER, B. *Aplikácia metódy viackriteriálneho rozhodovania v krízovom riadení* [online]. ŽU v Žiline: FBI. Dostupné z: http://fbi.uniza.sk/ktvi/leitner/2_predmety/OA/00_Priblizne_riesenie_AHP.pdf

[7] *Fyzická a objektová bezpečnosť* [online]. Národný bezpečnostný úrad. Dostupné z: http://www.nbu.gov.sk/ochrana-utajovanych-skutocnosti/povinnosti-a-moznosti/fyzicka-a-objektova-bezpecnost/index.html

[8] JANOŠCOVÁ, R. 2014 [online]. *Princípy informačnej bezpečnosti*. Dostupné z: http://ics.upjs.sk/~jirasek/ops/Janoscova.pdf

[9] FERRAIOLO, D., KUHN, R., CHANDRAMOULI, R. 2007 [online]. *Role-based Access Control*. ISBN 978-1-59693-113-8.

[10] *Personálna bezpečnosť* [online].Bezpečnostná študovňa. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/personalna-bezpecnost-87e.html

[11] *Princíp biomerie*. [online]. Biometria. Dostupné z: http://www.biometria.sk/principy-biometrie.html

[12] *Žiletkový drát* [online]. Levné oplocení. Dostupné z: https://www.levne-oploceni.cz/ziletkovy-drat-730-mm.html

[13] SKALICKÁ, P., 2017. Ochrana kritické infrastruktury – případová studie. In: *Krízový manažment*. Roč. 16, č. 2, s.70-77. ISBN 1336-0019.

[14] ADAMÍKOVÁ, J., 2016. Východiska na analýzu rizík výpadku elektrickej energie. In: *Krízový manažment.* Roč. 15, č. 1 s.81-86. ISBN 1336-0019.