Smernica o identifikácii a odstraňovaní citlivých informácií v dokumentáciách pre sprístupnenie verejnosti

Článok 1
Účel smernice

Účelom smernice je určenie spôsobu identifikácie citlivých informácií v dokumentáciách určených pre sprístupnenie:

a) verejnosti podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov alebo
b) účastníkom konania podľa zákona č. 50/1976 Zb. o územnom plánovaní a stavebnom poriadku (stavebný zákon) v znení neskorších predpisov alebo zákona č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov určených v § 8 ods. 2 atómového zákona

a jej následné odstraňovanie v týchto dokumentáciách ako aj definovanie indikátorov a argumentov na podporu rozhodnutia, že príslušná informácia je citlivá.

Článok 2
Oblasť platnosti

Smernica platí pre všetkých zamestnancov úradu, ktorí sa podieľajú na identifikácii a následnom odstraňovaní citlivých informácií v dokumentáciách určených v Článku 1 tejto smernice.

Článok 3
Všeobecná časť, vymedzenie pojmov

1. Vzhľadom na globálnu bezpečnostnú situáciu úrad rovnako ako aj mnohé ďalšie dozorné orgány vo svete považuje za nevyhnutné určiť informácie, ktoré sa nemôžu sprístupniť verejnosti, aby nedošlo k využitiu informácií na zlovoľné aktivity.

   Citlivá informácia je zadefinovaná v zákone č. 350/2011 Z. z., ktorým sa mení a dopĺňa zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v § 3 ods. 16 nasledovne: „Za dokumentáciu obsahujúcu citlivé informácie sa považuje dokumentácia, ktorej zverejnenie by sa mohlo použiť na naplánovanie a vykonanie činností s cieľom spôsobiť narušenie alebo zničenie jadrového zariadenia a tým nepriaznivo ovplyvniť bezpečnosť verejnosti[1)] a spôsobiť ekologickú alebo ekonomickú škodu. Táto dokumentácia sa sprístupňuje po vylúčení citlivých informácií.“.
   Každá žiadosť o informácie sa posudzuje individuálne. Obmedzenie prístupu k citlivým informáciám v zmysle vyššie uvedenej definície sa posudzuje reštriktívnym spôsobom, berúc do úvahy verejný záujem na zverejnení informácií o životnom prostredí a súvis s emisiami do životného prostredia.

2. Informácie o životnom prostredí tak ako sú definované v článku 2 ods. 3 Aarhuského dohovoru (týkajúce sa najmä emisií do životného prostredia, údaje o množstve a zložení rádioaktívnych odpadov) sa musia zverejniť bez obmedzenia. V prípade, ak sa žiadosť

[1)] Čl. 4 ods. 4 Dohovoru o prístupe k informáciám, účasti verejnosti na rozhodovacom procese a prístupe k spravodlivosti v záležitostiach životného prostredia (oznámenie č. 43/2006 Z. z.).

o informácie týka dokumentácie, ktorá nemôže byť zverejnená bez obmedzenia, sprístupnia sa informácie o životnom prostredí po odstránení tých informácií, ktoré nemôžu byť zverejnené z bezpečnostných dôvodov. Informácie o životnom prostredí podľa článku 2 ods. 3 Aarhuského dohovoru sú najmä informácie v písomnej, obrazovej, zvukovej, elektronickej alebo inej materiálnej forme

a) o stave zložiek životného prostredia, ako sú ovzdušie a atmosféra, voda, pôda, krajina, krajinné a prírodné prostredie, biologická rôznorodosť a jej zložky vrátane geneticky modifikovaných organizmov a vzájomných vzťahov týchto zložiek;
b) o činiteľoch, ako sú látky, energia, hluk a žiarenie, a činnostiach a opatreniach vrátane administratívnych opatrení, dohôd v oblasti životného prostredia, politík, právnych predpisov, plánov a programov, ktoré ovplyvňujú alebo by mohli ovplyvniť zložky životného prostredia v rozsahu písmena a) a analýzy prínosov a nákladov a iných ekonomických analýz a odhadov používaných v rozhodovacom procese o životnom prostredí;
c) o stave zdravia a bezpečnosti obyvateľstva, podmienkach života obyvateľstva, kultúrnych pamiatkach a sídelných štruktúrach v rozsahu, v akom sú alebo môžu byť ovplyvnené stavom zložiek životného prostredia alebo prostredníctvom týchto zložiek činiteľmi, činnosťami alebo opatreniami uvedenými v písmene b).

3. Informáciou o životnom prostredí podľa § 2 ods. 1 písm. a) zákona č. 205/2004 Z. z. o zhromažďovaní, uchovávaní a šírení informácií o životnom prostredí a o zmene a doplnení niektorých zákonov je aj akákoľvek informácia v písomnej, obrazovej, zvukovej, elektronickej alebo inej materiálnej forme
   a) o stave významných biotopov prírodného prostredia, ako sú mokrade, morské pobrežné biotopy a ďalšie biotopy voľne žijúcich rastlín a voľne žijúcich živočíchov,
   b) o faktoroch, ako sú odpady vrátane rádioaktívnych odpadov, emisie a iné uvoľňovanie znečisťujúcich látok do životného prostredia, ktoré znečisťujú, ovplyvňujú alebo by mohli ovplyvniť zložky životného prostredia zložiek životného prostredia, ako sú ovzdušie, voda, pôda, horninové prostredie, významné biotopy prírodného prostredia, ako sú mokrade, morské pobrežné biotopy a ďalšie biotopy voľne žijúcich rastlín a voľne žijúcich živočíchov,
   c) o činnostiach a opatreniach vrátane administratívnych opatrení, predpisoch, politikách, plánoch, programoch a dohodách vo veciach životného prostredia, ktoré ovplyvňujú alebo môžu ovplyvniť zložky životného prostredia alebo faktory uvedené v písmene a) a b), ako aj o činnostiach a opatreniach na ochranu týchto zložiek,
   d) o správach o aplikácii a plnení podmienok všeobecne záväzných právnych predpisov na úseku starostlivosti o životné prostredie,
   e) o analýzach nákladov a prínosov a o ďalších analýzach a podkladoch ekonomického charakteru používaných v rámci opatrení a činností uvedených v písmene c) alebo
   f) o stave zdravia a bezpečnosti osôb vrátane prípadnej kontaminácie potravinového reťazca, o fyzikálnych, chemických a biologických faktoroch životného prostredia vo vzťahu k zdraviu ľudí, o kultúrnych lokalitách a sídelných štruktúrach, ak sú alebo môžu byť dotknuté v dôsledku stavu zložiek životného prostredia alebo cez tieto zložky z hociktorého z dôvodov uvedených v písmene b) a c).

4. Dokumentácia obsahujúca nasledovné informácie sa považuje za dokumentáciu obsahujúcu citlivé informácie podľa Článku 3 ods. 1 tejto smernice:
   a) identifikácia a označenie zariadení a stavieb, čísla miestností a popis lokality, kde sa nachádzajú,
   b) opis, parametre a označenie zariadení a technológií,

c) zdroje a miesto ich uloženia,
d) čísla a opis technologických celkov,
e) kategória seizmickej odolnosti,
f) funkcionalita, parametre a komponenty systému a jeho zálohovanie,
g) systémy riadenia a regulácie,
h) pomocné systémy pre bezpečnostné systémy, napr. systémy sekundárneho chladenia, dieselové systémy, systémy požiarnej vody,
i) napájanie: Všeobecné usporiadanie, riadenie, distribúcia.

Dokumentácia sa sprístupňuje po odstránení informácií, ktoré je možné považovať za citlivé informácie v zmysle Článku 3 ods. 1 smernice. Umožňuje sa prístup k informáciám z dokumentácie, ktoré je možné považovať za informácie o životnom prostredí v zmysle Článku 3 ods. 2 a ods. 3 smernice a ktoré zároveň nie je možné považovať za citlivé informácie v zmysle Článku 3 ods. 1 smernice. Každá žiadosť o informácie sa posudzuje individuálne, pričom akékoľvek obmedzenie prístupu k informáciám, ktoré sú z bezpečnostných dôvodov považované za citlivé informácie, je posudzované reštriktívnym spôsobom, berúc do úvahy verejný záujem na sprístupnení informácií o životnom prostredí a súvis s emisiami do životného prostredia.

5. Smernica stanovuje podmienky, ktoré budú použité na určenie citlivej informácie, ktorá nebude sprístupnená subjektom uvedeným v Článku 1 tejto smernice aby tak nedošlo k nechcenému poskytnutiu informácií tým, ktorí ich budú chcieť zneužiť na zlovoľné aktivity namierené voči jadrovým zariadeniam alebo jadrovým materiálom, prípadne možnému vykonaniu teroristického útoku.
6. Citlivé informácie sa týkajú celej škály informácií, ktorých strata, zneužitie, úprava alebo neoprávnený prístup môže ohroziť jadrovú bezpečnosť a fyzickú ochranu, a tým verejný záujem.
7. Informácie sú považované za citlivé vtedy, ak by ich zverejnenie mohlo mať jasný a významný prínos pre narušiteľov pre prípadný útok.
8. Rozsah nižšie uvedených citlivých informácií bol stanovený na základe analýzy a posúdenia možných zdrojov úniku citlivých informácií o jadrových zariadeniach, vo vzťahu ku fyzickej ochrane jadrových zariadení a práve konkrétna znalosť týchto detailných informácií by mohla byť rozhodujúca pri plánovaní zlovoľnej aktivity smerom k jadrovému zariadeniu alebo jadrovým materiálom. A naopak, absencia týchto informácií takéto zlovoľné konanie zásadným spôsobom komplikuje, ak nie vylučuje.
9. Argumentačná línia predstavuje kauzálny reťazec týkajúci sa všetkých argumentov, ktoré podporujú rozhodnutie o tom, že príslušná informácia je citlivá. Kauzálny reťazec tvoria fakty uvedené v jednotlivých prílohách smernice viažuce sa na príslušný typ citlivej informácie podľa katalógu.
10. Fyzickou ochranou (ďalej len „FO“) sa rozumie súbor technických, režimových alebo organizačných opatrení potrebných na zabránenie a zistenie neoprávnených činností s jadrovými zariadeniami, jadrovými materiálmi, špeciálnymi materiálmi a zariadeniami, pri nakladaní s rádioaktívnymi odpadmi, vyhoretým jadrovým palivom, pri preprave rádioaktívnych materiálov, ako aj neoprávneného vniknutia do jadrového zariadenia a vykonania sabotáže. [2])
11. Bezpečnostný systém ochrany (ďalej len „BeSy“) je súbor technických prostriedkov, technologických pravidiel, organizačných smerníc a spôsobu chovania sa ľudí (Security

[2]) § 2 písm. b) zákona č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Culture), ktorý synergickým pôsobením zabezpečuje bezpečný a projektovaný chod jadrového zariadenia, alebo skladovania, používania a manipulácie s jadrovými materiálmi.

12. Prekonanie účinnosti fyzickej ochrany (FO) a/alebo účinnosti bezpečnostných systémov (ochrany technológie) (BeSy) – „Prekonanie“ je také konanie útočníka, ktoré zabezpečí nepozorovanú manipuláciu bez viditeľného poškodenia zábran a ochranných mechanizmov. Detekčné systémy nemusia zaznamenať žiadnu aktivitu, lebo je legálna a vykonáva ju autorizovaný človek. Tak bude konať spravidla vnútorný páchateľ, ktorý je autorizovaný na vykonávanie určitej činnosti, ktorú však zneužije na konanie proti chránenému záujmu. Prekonaním je aj prípadná manipulácia s prevádzkovými predpismi s cieľom následne (napr. aj v budúcnosti) vyvolať krízovú situáciu.
13. Eliminácia ľudských zdrojov FO a/alebo BeSy – „Eliminácia“ – znamená ovládnutie, resp. obmedzenie (vydieraním, hrozbou násilia, alebo násilím resp. usmrtením) činnosti človeka – pracovníka, obsluhy zariadenia, člena FO a iného zamestnanca.
14. Vyradenie systémov FO a alebo BeSy – „Vyradenie“ je konanie útočníka s cieľom vyradiť z prevádzky technické prostriedky FO a/alebo BeSy, resp. znemožniť fungovanie procesov FO a/alebo BeSy, pričom útočník prekonáva ochranné opatrenia pozorovane, t.j. existuje informácia o jeho konaní.
15. Obmedzenie účinnosti FO a/alebo BeSy – „Obmedzenie“ – je čiastočné narušenie funkčnosti prostriedkov a procesov FO a/alebo BeSy. Konanie útočníka je detekovateľné.
16. Citlivé informácie budú zo sprístupňovanej dokumentácie odstránené spôsobom, že uvedené informácie v dokumentácii zostanú, avšak budú odstránené takým spôsobom, aby boli nečitateľné.

3.1 Dokumentácia obsahujúce citlivé informácie podľa atómového zákona

Podľa § 3 ods. 17 atómového zákona sa za dokumentáciu obsahujúcu citlivé informácie rozumie dokumentácia uvedená v prílohe č. 1 bode A písm. c), bode B písm. a), b), i), m), bode C písm. a), d), i), j), s), w) a prílohe č. 2 bode A písm. b), bode B písm. b) atómového zákona, ktorými sú:

1. projektový zámer na fyzikálno-technické riešenie jadrového zariadenia v úrovni zadávacieho projektu,
2. predbežná bezpečnostná správa, ktorá preukazuje plnenie zákonných požiadaviek na jadrovú bezpečnosť na základe údajov, o ktorých sa uvažuje v projekte,
3. projektová dokumentácia potrebná k stavebnému konaniu,
4. predbežné limity a podmienky bezpečnej prevádzky,
5. dokumentácia podľa § 6 ods. 2 písm. j) zákona č. 541/2004 Z. z. v znení neskorších predpisov,
6. limity a podmienky bezpečnej prevádzky,
7. program uvádzania jadrového zariadenia do prevádzky členený na etapy,
8. predprevádzková bezpečnostná správa, ktorá spresňuje správu uvedenú v bode B písm. a),
9. pre jadrové zariadenia s jadrovým reaktorom pravdepodobnostné hodnotenie bezpečnosti prevádzky pre odstavený reaktor a pre nízke výkonové hladiny, ako aj pre plný výkon reaktora,
10. doklady o pripravenosti jadrového zariadenia na uvádzanie do prevádzky, pre skúšobnú prevádzku správa o vyhodnotení uvádzania jadrového zariadenia do prevádzky a pre trvalú prevádzku správa o vyhodnotení skúšobnej prevádzky,
11. druh a množstvo rádioaktívnych materiálov určených na prepravu,
12. druh a množstvo jadrových materiálov, ktoré majú byť dovezené alebo vyvezené, druh a množstvo špeciálnych materiálov a zariadení, ktoré majú byť vyvezené.

3.2 Citlivé informácie

Typické citlivé informácie nezverejňované napr. pri stavebnom konaní, správnom konaní, atď. podľa ustanovenia čl. 4 ods. 4 písm. b) Aarhuského dohovoru o výlukách z poskytovania informácií z dôvodu možného nepriaznivého ovplyvnenia bezpečnosti verejnosti je možné rozdeliť do nasledovných skupín:

1) Vymenované informácie o:
   a) fyzickej ochrane, ktoré nie sú utajované podľa zákona č. 215/2004 Z. z.,
   b) preprave jadrových materiálov, ktoré nie sú utajované podľa zákona č. 215/2004 Z. z. /4/,
   c) preprave rádioaktívnych odpadov, ktoré nie sú utajované podľa zákona č. 215/2004 Z. z. /4/,
   d) rozmiestnení HW prostriedkov bezpečnostných systémov kontroly a riadenia a systémov kontroly a riadenia so vzťahom k bezpečnosti,
   e) verziách SW, ktorý je súčasťou vybraných zariadení (napr. SKR),
   f) bezpečnostných systémoch,
   g) grafických častiach zoznamov vybraných zariadení a zoznamov seizmicky klasifikovaných zariadení,
   h) operatívnych schémach systémov jadrových zariadení.

2) Informácie o zariadeniach:
   a) napájanie I. a II. kategórie systému zaisteného napájania.

3) Informácie o analýzach, výpočtoch, výsledkoch:
   a) pravdepodobnostných analýz (PSA),
   b) pevnostných výpočtov,
   c) analýzy rizík.

4) Informácie o funkcionalite:
   a) napájania I. a II. kategórie zaisteného napájania vlastnej spotreby,
   b) systému riadenia bezpečnostných systémov,
   c) systému kontroly bezpečnostných systémov,
   d) spojenia obsluhy jadrového zariadenia s havarijnými štábmi.

5) Informácie o umiestnení:
   a) zariadení,
   b) objektov,
   c) zariadenia pre prívod surovej vody do elektrárne,
   d) jadrových materiálov,
   e) rádioaktívnych odpadov,
   f) vzduchotechnických zariadení a prívodov pitnej vody,
   g) vstupov do objektu (vrátane počtu),
   h) chemikálií,
   i) bezpečnostných systémov,
   j) napájania vlastnej spotreby a vyvedenia výkonu.

6) Informácie o opise, popise, označení:
   a) budov,
   b) miestností,
   c) potrubných kanálov,
   d) okolia budov,
   e) počte budov, podlaží,
   f) schémach blokovej dozorne,
   g) podrobnom opise IT systémov,
   h) podrobnom opise funkcií bezpečnostných systémov,
   i) podrobnom popise systémov riadenia, kontroly a pod.,
   j) označovaní DPS,
   k) napájaní I. a II. kategórie systému zaisteného napájania,
   l) napájaní vlastnej spotreby a vyvedenia výkonu,
   m) bezpečnostných systémov,
   n) vzduchotechnických zariadení a prívodov pitnej vody,
   o) systémoch požiarnej signalizácie a hasenia.

7) Informácie o zoznamoch a deklaráciách množstiev:
   a) jadrových materiálov,
   b) rádioaktívnych odpadov,
   c) vzduchotechnických zariadení a prívodov pitnej vody,
   d) chemikálií,
   e) napájaní I. a II. kategórie systému zaisteného napájania.

8) Informácie nepriamo identifikujúce osoby – pracovníkov jadrových zariadení a osôb vykonávajúcich fyzickú ochranu jadrového zariadenia dodávateľským spôsobom:

   a) osobné údaje nespadajúce do kompetencie zákona o ochrane osobných údajov umožňujúce identifikáciu osoby s pracovnou pozíciou (blahoželania v podnikovej tlači, články o osobe pri rôznych príležitostiach, prezenčné listiny, evidenčné zoznamy a pod.),
   b) názvy pracovných pozícií a ich náplň, najmä v čase neštandardnej prevádzky jadrového zariadenia,
   c) zoznamy príslušníkov ochrannej zmeny slúžiace na výkon služby ochrany jadrového zariadenia (výdaj strojových náležitostí, plány dovoleniek, evidencia gastrolístkov a pod.)

3.2.1 Indikátory citlivosti informácie

Na bezpečnosť jadrových zariadení a materiálov, majú vplyv rôzne činitele. Hlavnými a rozhodujúcimi sú fyzická ochrana a bezpečnostné systémy (súbor technických prostriedkov, technologických pravidiel, organizačných smerníc a spôsobu chovania sa ľudí (Security Culture), ktorý synergickým pôsobením zabezpečuje bezpečný a projektovaný chod jadrového zariadenia, alebo skladovania, používania a manipulácie s jadrovými materiálmi).

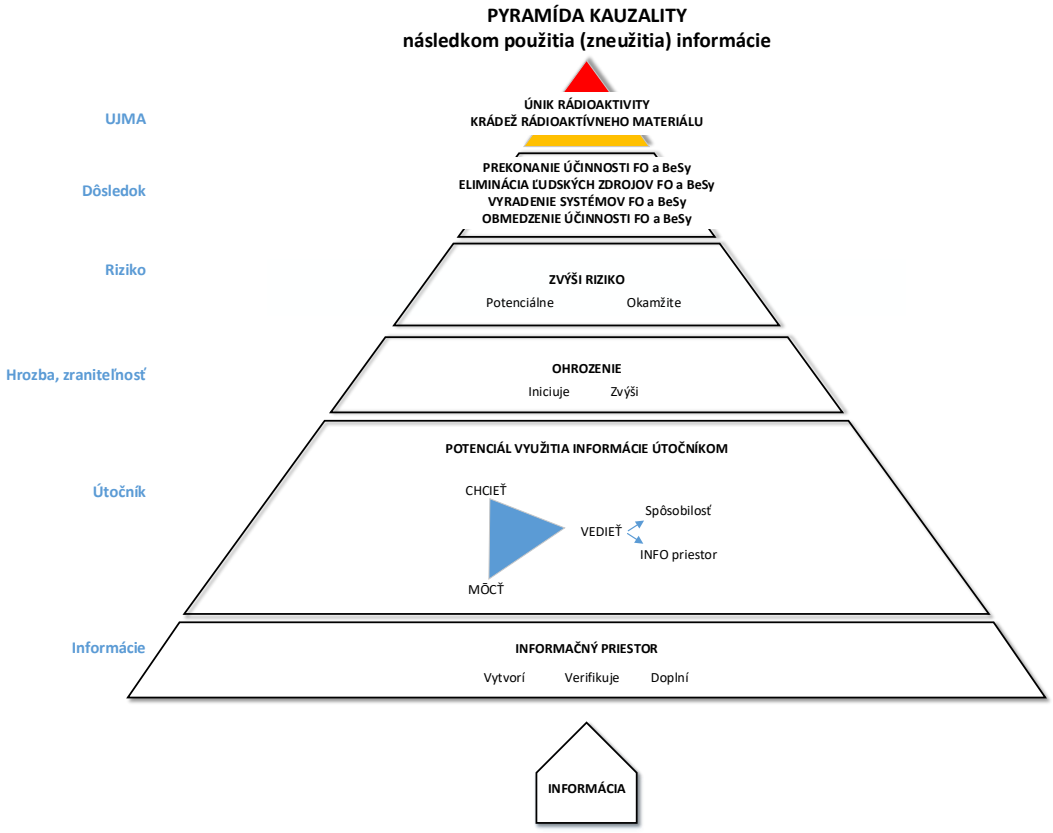
Fyzická ochrana zabezpečuje fyzickú a objektovú ochranu, t.j. predovšetkým izoláciu areálov kde prebiehajú procesy jadrového priemyslu (jadrové zariadenia, sklady jadrových materiálov a pod.).

Bezpečnostné systémy zabezpečujú najmä fungovanie technologických prvkov a uzlov v projektovaných parametroch tak, aby bola zabezpečená hlavná funkcionalita zariadenia jadrového priemyslu (chod jadrového reaktora, skladovanie, spracovanie a prepracovanie jadrového materiálu a pod.).

Kategorickou ujmou v prostredí jadrového priemyslu je:

a) únik rádioaktivity,
b) krádež rádioaktívneho materiálu.

Z hľadiska časového a vecného vývoja situácie, ktorá potenciálne môže viesť k popísanej ujme, je potrebné analyzovať jednotlivé etapy vývoja krízovej situácie.



Obrázok č.1 Pyramída kauzality

Obrázok č.1 popisuje kauzálny reťazec. Ľubovoľná informácia môže vytvoriť, verifikovať, alebo doplniť informačný priestor o danej vec, alebo jave.

Útočník potrebuje na dokonanie svojho úmyslu tri komponenty: motiváciu (Chcieť), podmienky (Môcť) a musí Vedieť, t. j. musí mať určité spôsobilosti (zručnosti, vedomosti) a informačný priestor.

V závislosti od potenciálu – schopnosti útočníka tento informačný priestor využiť na páchanie trestného činu, môže útočník vygenerovať ohrozenie, alebo existujúce ohrozenie

zväčšiť, čím sa prirodzene môže okamžite, alebo potenciálne zvýšiť riziko pre chránený záujem.

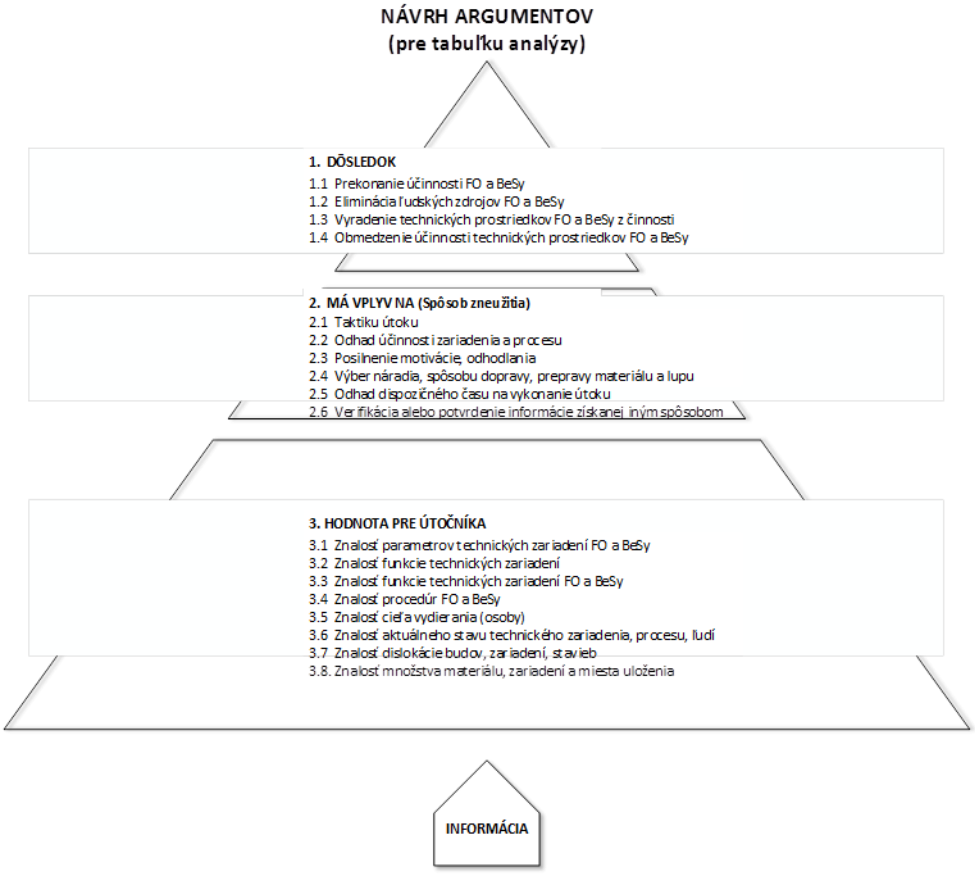
3.2.2 Argumenty

Pre exaktné stanovenie, že posudzovaná informácia môže byť, resp. je citlivá, potrebujeme súbor argumentov, ktoré podporia toto rozhodnutie.

Vychádzajúc z predošlej analýzy indikátorov, je možné rozdeliť proces hľadania argumentov na tri etapy:

a) nájsť odôvodnenie, prečo je informácia, indikovaná ako citlivá, dôležitá pre útočníka – akú má pre neho a jeho konanie hodnotu,
b) aký má predmetná informácia vplyv na rozhodovanie, alebo konanie útočníka, t. j. aký môže byť dôsledok jej použitia (zneužitia),
c) aká môže nastať ujma v prípade, že predmetná informácia útočníkom, bude náležitým spôsobom použitá.

Túto situáciu graficky znázorňuje Obrázok č.2.



Obrázok č. 2 Návrh súboru argumentov

Dané argumenty sú použité na odôvodnenie oprávnenosti prehlásiť príslušné informácie uvedené v tejto smernici v bode 3.2 za citlivé.

3.2.2.1 Hodnota pre útočníka

Parameter „Hodnota pre útočníka“ vyjadruje morfologickú (obsahovú), syntaktickú a sémantickú hodnotu informácie, ku ktorej sa útočník dostal najrôznejším spôsobom. Hodnota môže vzniknúť, predstavovať doplnenie alebo potvrdenie predtým získanej informácie. Útočník môže použitím metód asociácie, integrácie, dedukcie a indukcie získať nový obsah poznania a to z informácií, ktoré samostatne predstavujú absolútne „nič nehovoriaci“ obsah.

Medzi takéto môžeme zaradiť informácie, ktoré poskytnú útočníkovi najmä:

1. Znalosť parametrov technických zariadení FO a BeSy

Aj keď väčšina informácií o fyzickej ochrane je v režime utajovaných skutočností, je nenulové riziko, že týchto informácií sa môže útočník zmocniť dedukciou z neutajovaných informácií a fyzickej ochrane. Rovnaké pravidlo platí aj pre informácie o bezpečnostnom systéme. Znalosť procesov a parametrov umožní útočníkovi efektívne plánovať a vykonať útok s využitím slabín, alebo zneužitím informácií o projektovaných parametroch. Umožní mu plánovať typy náradia, prístrojov a iných pomôcok, ktoré bude potrebovať na prelomenie odporu.

2. Znalosť funkcie technických zariadení

Znalosť funkcie technických zariadení umožňuje útočníkovi naplánovať a vykonať útok proti technickým zariadeniam, výpadok ktorých môže spôsobiť tzv. „domino efekt“, t. j. že séria technických porúch a havárií vytvorí krízovú situáciu, ktorá môže zvýšiť riziko úniku rádioaktivity, resp. krádeže rádioaktívneho materiálu. Takýto typ útoku by mal charakter technickej poruchy, alebo havárie a za určitých okolností by dokázal zamaskovať skutočnosť, že išlo o plánovaný útok.

3. Znalosť funkcie technických zariadení FO a BeSy

Informácia umožňuje plánovanie efektívneho útoku s vyhnutím sa, alebo prekonaním zábran, ktoré vytvárajú prvky FO a BeSy.

4. Znalosť procedúr FO a BeSy

Informácia umožňuje plánovanie efektívneho útoku s vyhnutím sa, alebo prekonaním zábran, ktoré vytvárajú procedúry FO a BeSy.

5. Znalosť cieľa vydierania (osoby)

Túto informáciu môžu tvoriť napr. „nevinné“ články v podnikovej tlači, kedy je napr. jubilant pozdravený a identifikovaný menom a pracovným zaradením. Ďalej to môžu byť informácie bez uvedenia mena konkrétneho pracovníka, ale ktoré obsahujú informáciu, že napr. príslušný proces má vo funkčnej náplni názov pracovnej pozície.

6. Znalosť aktuálneho stavu technického zariadenia, procesu, ľudí

Typickou informáciou tohto typu je periodicita kontrol, najmä na záložných (redundantných) systémoch. Informácia o tom, že „pravidelné kontroly na zariadení sa vykonávajú 1x pol roka“ v kombinácií s informáciou o aktuálne vykonanej kontrole

dáva útočníkovi informáciu o tom, kedy najbližšie bude zariadené znovu v pozornosti obsluhy a teda, koľko času má na nerušenú prípravu napr. sabotáže. Citlivými sú aj informácie o tom, že na danom zariadení prebieha modernizácia a bude plne funkčné až v určitom termíne.

7. Znalosť dislokácie budov, zariadení a stavieb

Informácie tohto typu umožňujú útočníkovi orientáciu v areáli, kde sa nachádza chránený záujem. Typickými príkladmi sú orientačné mapky a tabule pre návštevy. Citlivými sú aj označenia budov a zariadení v spojitosti ich funkciou v systéme. Ďalej to môžu byť informácie o existencii (neexistencii) a spôsobe ochrany predmetnej budovy, alebo zariadenia.

8. Znalosť množstva materiálu, zariadení a miesta uloženia

Informácia spresňuje útočníkovi situáciu a podmienky pre páchanie jeho zámeru.

3.2.2.2 Spôsob zneužitia získaných informácií

Informácia, ktorú útočník získa, po spracovaní (vyhodnotenie, doplnenie a verifikácia predtým získaných informácií a pod.) môže mať vplyv na prípravu útoku alebo na vykonanie útoku, najmä na taktiku útoku. jeho bezprostredné konanie, alebo na prípravu útoku. Komponentmi, ktoré kategoricky ovplyvňujú taktiku útoku sú najmä:

1. Odhad účinnosti zariadenia a procesu

Informácie o účinnosti zariadenia a procesu umožnia útočníkovi odhadnúť intenzitu odporu, ktorý bude musieť prekonať alebo faktory, ktoré môžu byť pre neho nápomocné pre vykonanie útoku.

2. Posilnenie motivácie, odhodlania čin vykonať

Systematické vyhodnotenie získaných informácií a zváženie vlastných síl a prostriedkov v súvislosti s predpokladanými obrannými a ochrannými opatreniami, môžu zásadne ovplyvniť rozhodnutie útočníka čin vykonať a zároveň aj guráž, s ktorou útočník bude postupovať.

3. Výber náradia, spôsobu dopravy, prepravy materiálu a lupu

4. Odhad dispozičného času na vykonanie útoku

5. Verifikáciu alebo potvrdenie informácie získanej iným spôsobom.

3.2.2.3 Typy dôsledkov – ujmy

S obmedzením sa na podmienky jadrového priemyslu, môžeme hovoriť o týchto typoch ujmy:

a) prekonanie účinnosti fyzickej ochrany (FO) a/alebo účinnosti bezpečnostných systémov (ochrany technológie) (BeSy),

b) eliminácia ľudských zdrojov FO a/alebo BeSy,
c) vyradenie systémov FO a/alebo BeSy,
d) obmedzenie účinnosti FO a/alebo BeSy.

3.3 Analýza rizík podľa jednotlivých položiek uvedených v kapitole 3.2

Všetky položky uvedené v kapitole 3.2 boli následne podrobené analýze rizík. Analýza rizík bola vykonaná v štruktúre:

a) skupina informácií (podľa kapitoly 3.2),
b) opis obsahu informácie (jednotlivé podbody z kapitoly 3.2),
c) bližšia špecifikácia,
d) príklad. Táto časť analýzy bola zavedená s cieľom lepšie porozumieť obsahu a bližšej špecifikácii
e) hodnota pre útočníka. Hodnota pre útočníka bola identifikovaná s cieľom zistiť jednotlivé druhy hrozby a bola vykonaná podľa modelu (Obrázok č. 2):
   - znalosť parametrov technických zariadení FO,
   - znalosť parametrov technických zariadení BeSy,
   - znalosť funkcie technických zariadení,
   - znalosť funkcie technických zariadení FO,
   - znalosť technických zariadení BeSy,
   - znalosť procedúr FO,
   - znalosť procedúr BeSy,
   - znalosť cieľa vydierania,
   - znalosť aktuálneho stavu technického zariadenia,
   - znalosť aktuálneho stavu procesu,
   - znalosť aktuálneho stavu ľudských zdrojov,
   - znalosť dislokácie budov, zariadení a stavieb,
   - znalosť množstva materiálu, počtu zariadení a miesta uloženia,
   - kombinácia znalostí.
f) Spôsob zneužitia (Má vplyv na) (hľadal sa možný spôsob využitia informácie útočníkom) (Obrázok č. 2):
   - taktika útoku,
   - odhad účinnosti zariadenia a procesu,
   - posilnenie odhodlania konať,
   - výber náradia,
   - výber spôsobu dopravy,
   - výber spôsobu prepravy materiálu a lupu,
   - odhad dispozičného času na vykonanie útoku,

- verifikácia alebo potvrdenie informácie získanej iným spôsobom.

g) Dôsledok (Obrázok č. 2) – ujma v zmysle Pyramídy kauzality Obrázok č.1:
   - prekonanie účinnosti FO,
   - prekonanie účinnosti BeSy,
   - eliminácia ľudských zdrojov FO,
   - eliminácia ľudských zdrojov BeSy,
   - vyradenie technických prostriedkov FO z činnosti,
   - vyradenie technických prostriedkov BeSy z činnosti,
   - obmedzenie účinnosti technických prostriedkov FO,
   - obmedzenie účinnosti technických prostriedkov BeSy,
   - kombinácia dôsledkov.

Výsledky Analýzy rizík jednotlivých položiek nachádzajúcich sa v bode 3.2 sú uvedené v Prílohe č.2.

Vykonaná Analýza rizík potvrdila oprávnenosť jednotlivých položiek Smernice uvedených v bode 3.2.

3.4 Vypracovanie argumentačného aparátu

Pre jednotlivé položky uvedené v bode 3.2 je vypracovaný argumentačný aparát na potvrdenia oprávnenosti považovať jednotlivé informácie za citlivé.

Postupuje sa podľa tohto algoritmu:

a) vypracovanie zoznamu skupín citlivých informácií v oblasti technológie, procesov a ľudského faktora,
b) vypracovanie Analýzy rizík pre jednotlivé skupiny citlivých informácií,
c) vypracovanie argumentačných línií a ich redukcia na prakticky použiteľný rozsah.

3.4.1 Vypracovanie kategórií skupín citlivých informácií

Kategórie skupín citlivých informácií v týchto oblastiach:
a) Technológia – citlivé informácie popisujúce tie časti a parametre technológie, ktoré môžu viesť ku zvýšeniu rizika.
b) Procesy – citlivé informácie o existencii a obsahu procesov, ktoré môžu viesť ku zvýšeniu rizika.
c) Ľudský faktor – informácie zdanlivo neškodné, ale ktoré sú svojim obsahom a najmä kontextom s inými informáciami citlivé informácie.

3.4.2 Vypracovanie Analýzy rizík pre jednotlivé skupiny citlivých informácií

Pre jednotlivé skupiny citlivých informácií bola vypracovaná analýza rizík v zostave:

a) kategória (technologické, procesy, ľudský faktor),
b) kód (identifikátor prakticky použiteľný v ďalšom spracovaní cieľa práce),
c) skupiny citlivých informácií (relatívne presná špecifikácia obsahu informácie, ktorá je citlivá),
d) hodnota pre útočníka – nosič rizika. Predstavuje úžitok, ktorý získanie predmetnej informácie poslúži útočníkovi k naplánovaniu a vykonaniu útoku,
e) využitie z pohľadu útočníka,
f) negatívny dôsledok – popis čo môže byť dôsledkom zneužitia citlivej informácie útočníkom,
g) riziko (odhad na škále „Vysoké – Stredné – Nízke“. Ide o expertný, ale subjektívny odhad.

Úplné výsledky analýzy rizík pre jednotlivé skupiny informácií je uvedený v Prílohe č.3. Analýzou rizík vznikol Katalóg citlivých informácií rozčlenených do kategórií.

3.4.3 Vypracovanie argumentačných línií a ich redukcia na prakticky použiteľný rozsah

Poslednou časťou argumentácie je vypracovanie argumentačných línií pre ich praktické využitie na preukázanie oprávnenosti pri označovaní informácií v dokumentácií za citlivé.

Rozdelenie argumentov do troch kategórií a niekoľko skupín je uvedené v Prílohe č.4. Z Prílohy č.4 vyplýva, že v kategórii:

a) technológia sa identifikovalo celkom 12 skupín citlivých informácií,
b) procesy sa identifikovalo celkom 9 skupín citlivých informácií,
c) ľudský faktor sa identifikovala 3 skupiny citlivých informácií.

Uvedená štruktúra je pomerne neprehľadná. Z toho dôvodu bolo potrebné nájsť ďalšie prvky zhody, resp. podobnosti, aby sa zredukoval celkový počet. Redukcia je farebne vyznačená v Prílohe č.5. Následnou argumentáciou a spresnením jednotlivých skupín a ich znenia vznikli redukované argumentačné línie uvedené v Prílohe č.6.

Rozdelenie uvedené v Prílohe č.6 je použiteľné pre argumentáciu, prečo je príslušná informácia považovaná za citlivú.

Článok 4
Procesy, činnosti, zodpovednosti

1. Príjem a zaevidovanie žiadosti o poskytnutie resp. sprístupnenie informácií alebo dokumentácie.
   Zodpovedný: sekretariát úradu

2. Pridelenie žiadosti o poskytnutie resp. sprístupnenie informácií alebo dokumentácie na vybavenie vecne príslušnému odboru podľa Registratúrneho poriadku a registratúrneho plánu úradu /5/ a v spolupráci s Kanceláriou úradu.
   Zodpovední: vedúci zamestnanci.

3. Posúdenie či sa jedná o žiadosť o sprístupnenie dokumentácie s citlivými informáciami.
   Zodpovední: riaditeľ vecne príslušného odboru.

4. Určenie zamestnanca zodpovedného za odstraňovanie citlivých informácií, prípadne poskytnutie ďalších inštrukcií na vybavenie podania.
   Zodpovedný: riaditeľ vecne príslušného odboru.

5. V prípade, že posudzovanie dokumentácie si vyžaduje spoluprácu viacerých špecialistov v rámci odboru, viacerých odborov úradu alebo externej organizácie, zváži riaditeľ vecne príslušného odboru potrebu a rozsah tejto spolupráce.
   Zodpovedný: riaditeľ vecne príslušného odboru.

6. Spolupráca špecialistov v rámci úradu sa vždy vyžiada vnútorným listom, ku ktorému je priložená príslušná časť dokumentácie.
   Zodpovedný: riaditeľ vecne príslušného odboru.

7. Posúdenie dokumentácie externou organizáciou sa vykoná na základe obchodnoprávnej zmluvy s oprávnenou osobou a jej odborného hodnotenia.
   Zodpovedný: riaditeľ vecne príslušného odboru.

8. Vytvorenie kópie dokumentu, v ktorej sa identifikujú a odstraňujú citlivé informácie v súlade s bodom 3.2. tejto smernice.
   Zodpovedný: určený zamestnanec

9. Kontrola odstránenej citlivej informácie/dokumentácie.
   Zodpovedný: riaditeľ vecne príslušného odboru.

10. Zaslanie dokumentu s odstránenými citlivými informáciami Kancelárii úradu vnútorným listom.
    Zodpovedný: určený zamestnanec

11. Vypracovanie odpovede na žiadosť o poskytnutie/sprístupnenie informácií/dokumentácie a zaslanie informácií/dokumentu žiadateľovi.
    Zodpovedný: Kancelária úradu

12. Zaslanie rovnopisu odoslanej odpovede určenému zamestnancovi vnútorným listom.
    Zodpovedný: Kancelária úradu

13. Založenie rovnopisu zaslanej dokumentácie/informácie do spisu.
    Zodpovedný: určený zamestnanec

Článok 5
Ciele kvality

Nie sú stanovené.

Článok 6
Organizačné zabezpečenie

1. Za organizačné zabezpečenie odstraňovanie citlivých informácií v dokumentáciách pre sprístupnenie verejnosti zodpovedá riaditeľ odboru, do ktorého kompetencií daná dokumentácia patrí.

2. Dotknutí zamestnanci úradu postupujú pri identifikácii a odstraňovaní citlivých informácií v súlade s predmetnou smernicou.

3. Za kontrolu dodržiavania tejto smernice zodpovedá riaditeľ odboru, do ktorého kompetencií daná dokumentácia patrí.

Článok 7
Súvisiace dokumenty

1. Čl. 4 ods. 4 Dohovoru o prístupe k informáciám, účasti verejnosti na rozhodovacom procese a prístupe k spravodlivosti v záležitostiach životného prostredia (oznámenie č. 43/2006 Z. z.).

2. § 11 ods. 1 písm. i) zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.

3. Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

4. Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

5. Registratúrny poriadok a registratúrny plán ÚJD SR.

Článok 8
Zrušovacie ustanovenie

Zrušuje sa Smernica o identifikácii a odstraňovaní citlivých informácií v dokumentáciách pre sprístupnenie verejnosti S 330 017:19, č. 4342/2019 zo dňa 14. 6. 2019.

Článok 9
Použité skratky

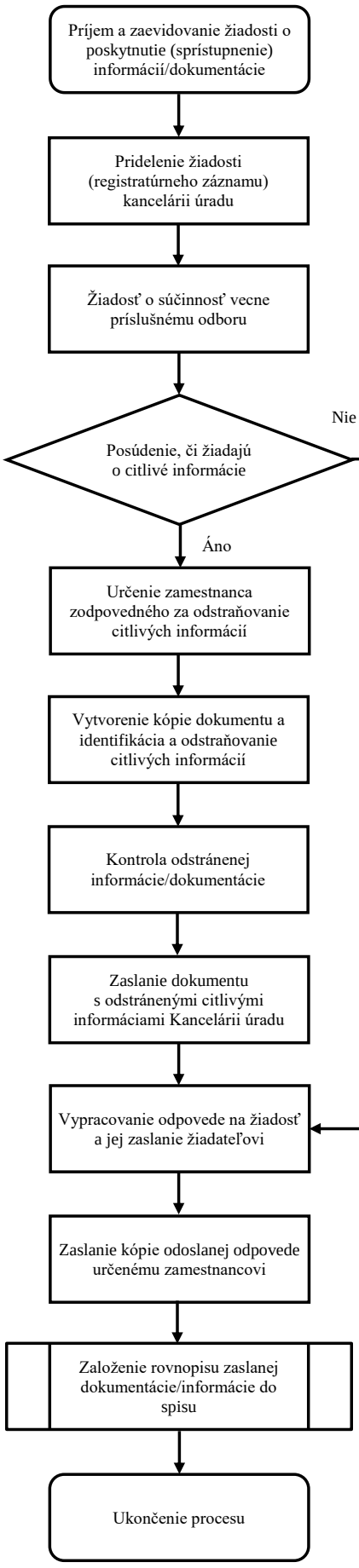
BeSy – bezpečnostný systém ochrany
DPS – čiastkový prevádzkový systém
FO – fyzická ochrana

HW – hardvér
PSA – pravdepodobnostná analýza
SKR – systémy kontroly a riadenia
SW – softvér

Článok 10
Prílohy

Príloha č.1: Vývojový diagram
Príloha č.2: Analýza indikátorov a argumentov
Príloha č.3: Analýza rizík a katalóg citlivých informácií
Príloha č.4: Rozdelenie argumentov do troch kategórií a niekoľko skupín
Príloha č.5: Redukcia kategórií a skupín
Príloha č.6: Redukované argumentačné línie

Príloha č.1: Vývojový diagram



1. Podateľňa
2. Zodpovedný zamestnanec KÚ
3. Zodpovedný zamestnanec KÚ
4. Riaditeľ vecne príslušného odboru
5. Riaditeľ vecne príslušného odboru
6. Určení zamestnanci úradu
7. Riaditeľ vecne príslušného odboru
8. Určení zamestnanci úradu
9. Zodpovedný zamestnanec KÚ
10. Zodpovedný zamestnanec KÚ
11. Určení zamestnanci úradu