ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA BEZPEČNOSTNÉHO INŽINIERSTVA

KRÍZOVÝ MANAŽMENT - 1/2015

CITLIVÉ INFORMÁCIE

SENSITIVE INFORMATION

Jaroslav SIVÁK[1]

SUMMARY:

The term "sensitive information" is used in practice under the legal standards (Law standards) of the Slovak Republic and also in daily language. In the second of these cases it is often the use of the term without deeper knowledge (or without knowledge about background) respectively without deeper understanding. From analysis of laws of the Slovak Republic in this specific area we can find out insufficient definition of the term "sensitive information". The absence of definition causes problems in the security practice of designation of the relevant information as "sensitive" and consequently during manipulation (operation) with them. The author present the analysis of proper use of the term "sensitive information" and, furthermore author try to establish definition of the term "sensitive information" within the broader context.

KEYWORDS: *sensitive information, classified information, harm, disclosure, definition of sensitive information*

ÚVOD

Informácia, z hľadiska bezpečnostného výskumu a bezpečnostnej vedy, predstavuje klasické aktívum. Samotná informácia, alebo spôsob nakladania s ňou, môže za určitých okolností vytvárať zdroj rizika. Tento stav môže vyústiť do určitej udalosti, ktorej dôsledky budú opísateľné dvoma základnými parametrami analýzy rizík, t.j. pravdepodobnosťou, že daná udalosť nastane (tým aj jej dôsledok) a mierou negatívneho dopadu (potenciálneho, alebo aktuálneho).

Správa sa stáva informáciou v dôsledku ľudskej interpretácie, alebo spracovaním pomocou algoritmov. Z uvedeného vyplýva, že citlivá informácia môže byť aj zdanlivo bezvýznamná informácia, ktoré ak nie je v danom kontexte, alebo nemá predchodcov, neobsahuje riziko.

Citlivosť informácie je parameter, ktorý určuje, prečo by sa mala tá, ktorá informácia ochraňovať a mal by sa obmedzovať okruh ľudí, ktorí by sa s ňom mohli oboznámiť a manipulovať s ňou. Tento základný parameter determinuje ujma, ktorá by nastala, keby sa citlivá informácia prezradila, nesprávne použila, získala, potenciálne, alebo aktuálne použila na negatívne, kriminálne závadové účely.

Základným posudzovaným a východiskovým faktorom je „zabrániť vzniku ujmy".

Následne vzniká legitímna otázka: Prezradenie, únik, ktorých informácií môžu viesť ku vzniku ujmy? Resp. ktoré informácie okrem zákonom taxatívne stanovených, môžu viesť ku stratám na ľudských životoch, ohrozeniu uzdravia, fatálnemu, kritickému zníženiu efektívnosti, ekonomickým, ekologickým a iným škodám a pod.?

Z podstaty pojmu „informácia" je zrejmé, že okrem explicitne vymenovaných kategórií informácií, existujú ďalšie, ktoré svojim informačným obsahom navonok nepôsobia ako informácie ohrozujúce, no v určitej konfigurácií, u určitej skupiny prijímateľov, za istých podmienok interpretácie sa môžu stať nebezpečnými.

Zákonné normy Slovenskej republiky chránia oprávnené záujmy prostredníctvom ochrany určitých kategórií informácií. Pokrytá je oblasť utajovaných skutočností, oblasť ochrany osobných údajov, obchodného tajomstva, no podstata citlivých informácií (napr. Zákon

[1] Jaroslav Sivák, doc. Ing. CSc., MBA, ALFA Security Technologies, a.s. , Dúbravská cesta 3, Bratislava, tel.: +421 903 706 805, e-mail: jsivak@alfasys.sk

č. 45/2011 Z. z. o kritickej infraštruktúre, Zákon č. 143/2013 Z. z. – „atómový zákon“) nie je dostatočne rozpracovaná.

Stav nedokonalého rozpracovania problematiky definovania, prípadne vymenovania citlivých informácií, zapríčinil zvýšený stupeň liberálneho pohľadu na význam a obsah informácií, čo má v danom prípade priamy vplyv na bezpečnosť.

Keďže zákonné normy Slovenskej republiky neobsahujú zoznamy explicitne vyjadrených skutočností, ktoré sú citlivou informáciou (s výnimkou zoznamov utajovaných skutočností predpísaných zákonom č. 215/2004 Z. z. v znení neskorších predpisov), bude potrebné odhaliť indikátory, ktoré určia citlivosť informácie.

1. SÚČASNÝ STAV V PRÁVNYCH NORMÁCH SLOVENSKEJ REPUBLIKY

Analýzou právnych noriem Slovenskej republiky, relevantných k predmetu skúmania, môžeme dospieť k týmto záverom:

1. Zákon o ochrane utajovaných skutočností 241/2001 Z. z. vymedzuje pojem „Utajovaná skutočnosť“ na základe ujmy, ktorú by Slovenska republika utrpela prezradením (zneužitím) takýchto informácii. Následne je pomerne presne upravený proces zaobchádzania s utajovanými skutočnosťami. Zákon vyžaduje, aby boli na príslušných úrovniach spracované aj relatívne presné zoznamy informácií, ktoré tvoria predmet utajovaných skutočností.
2. Okrem taxatívne vymedzenej skupiny utajovaných skutočností existuje skupina informácií označovaných ako „citlivé informácie“, ktoré sú o. i. predmetom zákonov:
   - zákon č. 143/2013 Z. z. o mierovom využívaní jadrovej energie,
   - zákon č. 45/2011 Z. z. o kritickej infraštruktúre.
3. Informácie, ktoré sú chránené vymedzeným spôsobom, alebo sú z kontextu „citlivé“ sú o. i. predmetom:
   - zákona č. 513/1991 Zb. - Obchodný zákonník,
   - zákona č. 122/2013 Z. z. o ochrane osobných údajov.

V praxi sa môžeme stretnúť s tým, že niektoré ústredné orgány štátnej správy používajú aj pojem „NEUVEREJŇOVAŤ“ na obmedzenie prístupu verejnosti k niektorým informáciám. Je to skôr pokyn, než označenie typu informácie podľa určitej klasifikácie.

V ďalšom texte vykonáme zjednodušenú analýzu týchto noriem z hľadiska pojmu „citlivá informácia“.

Zákon č. 241/2001 Z. z. o ochrane utajovaných skutočností sa zaoberá jasne vymedzenou oblasťou informácií, ktoré nazývame utajované skutočnosti. Nie je preto predmetom skúmania z hľadiska citlivých informácií.

Zákon č. 143/2013 Z. z. – atómový zákon, obsahuje pojem „citlivá informácia“.

V §3 odsek 14 zákona č. 541/2004 Z. z. sa uvádza: *„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 a spôsobiť ekologickú alebo ekonomickú škodu. Táto dokumentácia sa nezverejňuje podľa osobitného predpisu*.“ Ďalej zákon vymenúva dokumentáciu, ktorá môže obsahovať citlivé informácie.

Na základe uvedeného, je možné prehlásiť, že Zákon 143/2013 Z. z. nie je použiteľný na definíciu pojmu „citlivá informácia“. Definícia pojmu „citlivá informácia“ nie je uvedená. Zákon neobsahuje indikátory, podľa ktorých by bolo možne exaktne označiť, ktorá informácia je z hľadiska predmetného zákona citlivá. Existuje iba vymedzenie, kde sa citlivá informácia nachádza.

Zákonom č. 45/2011 Z. z. o kritickej infraštruktúre bol pojem „citlivá informácia“ v § 2, písm. k), vymedzený takto: „*citlivou informáciou o kritickej infraštruktúre (ďalej len „citlivá informácia“) neverejná informácia, ktorej zverejnenie by sa mohlo zneužiť na činnosť smerujúcu k narušeniu alebo zničeniu prvku.*“

Ďalej § 12 Citlivá informácia toho istého zákona upravuje spôsob nakladania s citlivou informáciou cit.: „§ 12 Citlivá informácia:

- Písomnosť alebo iný hmotný nosič, ktorý obsahuje citlivú informáciu, sa označuje slovami „Kritická infraštruktúra – nezverejňovať“.
- Oprávnená osoba je povinná zachovávať mlčanlivosť o citlivej informácii, a to aj po zániku jej oprávnenia oboznamovať sa s citlivou informáciou.

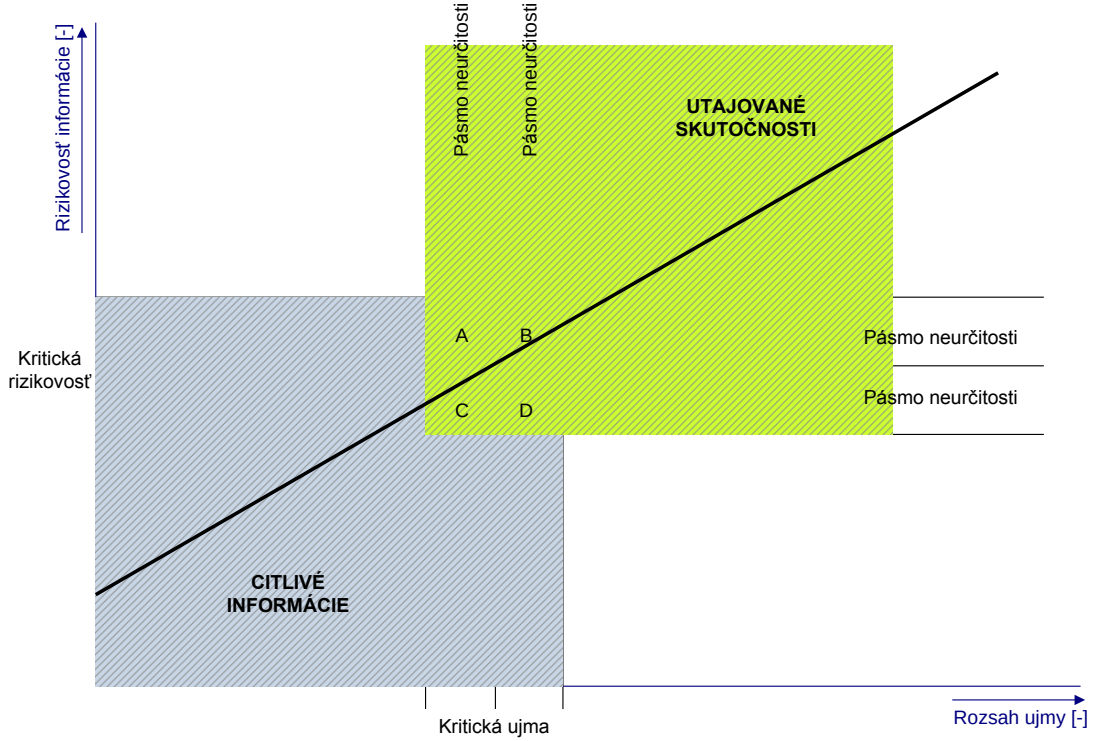
– Citlivá informácia sa nesprístupňuje podľa osobitného predpisu.“

Formulácia vo vyššie uvedených častiach zákona je prakticky nepoužiteľná pre účely identifikácie citlivosti informácie a pre určenie jej miery citlivosti. Samotný § 12 je úplne nepoužiteľný. V tejto podobe dovoľuje zákon rôznu interpretáciu procesu „zneužiť na činnosť smerujúcu k narušeniu alebo zničeniu prvku“, následkom čoho konkrétne osoby, ktoré majú rozhodovať o tom, ktorá informácia je citlivá, sú v stave nerozhodnosti.

V súvislosti so zákonom o kritickej infraštruktúre, vydalo Ministerstvo hospodárstva Slovenskej republiky Metodické usmernenie [4].

Príloha č. 4 obsahuje Zoznam citlivých informácií o kritickej infraštruktúre v pôsobnosti Ministerstva hospodárstva SR:

1. „Register prvkov kritickej infraštruktúry za rezort hospodárstva.
2. Oznámenie príslušného ústredného orgánu o rozhodnutí o určení prvku kritickej infraštruktúry a zaradení do sektora kritickej infraštruktúry.



Obrázok 1. **Vzťah utajovanej skutočnosti a citlivej informácie z hľadiska ujmy**

3. Oznámenie príslušného ústredného orgánu o rozhodnutí o určení prvku kritickej infraštruktúry a vyradení zo sektora kritickej infraštruktúry.
4. Bezpečnostný plán prevádzkovateľa prvkov kritickej infraštruktúry.
5. Analýza rizík príslušného sektora kritickej infraštruktúry.
6. Vyjadrenia k bezpečnostným plánom prevádzkovateľov.
7. Korešpondencia medzi prevádzkovateľom prvkov kritickej infraštruktúry a príslušným zodpovedným ústredným orgánom.
8. Informácie týkajúce sa ochrany prvkov kritickej infraštruktúry.“

Zoznam je v bodoch 1, 4, 5 a 8 plne použiteľný na účely manipulácie s informáciami, ktoré nie sú utajované, ale sú podľa zákona č. 45/2011 Z.z. označené ako „citlivé“. Ostatné body sú sporné, dokonca body 6 a 7 môžeme označiť za diletantstvo autora.

Zákon 45/2011 Z. z. nie je použiteľný na definíciu pojmu „citlivá informácia“.

Posledné dva zákony, ktoré boli analyzované, t.j. zákon č. 513/1991 Zb. Obchodný zákonník a zákon č. 122/2013 Z. z. o ochrane osobných údajov, pojem „citlivá informácia“ síce neobsahujú, ale popisujú istým spôsobom informácie, ktoré by nemali byť verejné.

2. VYMEDZENIE POJMU „CITLIVÁ INFORMÁCIA“

Oprávnenou otázkou je, že či nie je užitočné, z hľadiska klasifikácie informácií, pohybovať sa iba na úrovni dvoch stavov:
- verejná informácia,
- utajovaná skutočnosť,

pričom škála „Utajovaných skutočností“ už obsahuje dostatok stupňov na odlíšenie závažnosti podľa príslušnej ujmy.

Je vysoko pravdepodobné, že zavedenie pojmu „citlivá informácia“ bolo vynútené viac politickými a inými aspektmi ako odbornými argumentmi, najmä:
1. Nedostatočnou priepustnosťou systému udeľovania personálnych previerok na oboznamovanie sa s utajovanými skutočnosťami.
2. Neochotou niektorých zainteresovaných fyzických a právnických osôb podrobiť sa bezpečnostnej previerke.
3. Nedostatočným využitím existujúceho právneho systému v čase, keď vznikla kategória „citlivá informácia“.

Požaduje sa posúdiť vzájomný vzťah utajovanej skutočnosti a citlivej informácie prostredníctvom porovnania závažnosti jednotlivých typov ujmy. Prísne objektívne by sa mala posudzovať:
1. Veľkosť informácie meraná klasickými technickými metódami (entropia, množstvo informácie v bitoch a pod.).
2. Časové rozlíšenie potenciálu eskalácie krízovej situácie vplyvom úniku informácie a pod.

Obrázok 1 sa snaží objasniť, že je možné znázorniť vzťah medzi rizikovosťou informácie a veľkosťou (dôležitosťou) ujmy. Nech funkčný priebeh tejto závislosti je priamka (v skutočnosti ide o nelineárny vzťah, jeho charakter nebol vyšetrovaný).

Na základe určitých skutočností, je možné definovať kritickú ujmu a kritickú rizikovosť informácie, t.j. hranice rozdelenia informácie na utajovanú skutočnosť a citlivú informáciu. Je nesporné, že okolo oboch z týchto hraníc existuje určité tolerančné pásmo (sektory A, B, C a D). Jeho šírka a súmernosť voči kritickým hraniciam je daná najmä spornosťou v rozhodovaní. Je opodstatnené sa domnievať, že v skutočnosti bude, z titulu bezpečnosti (koeficientu bezpečnosti) toto tolerančné pásmo asymetrické, t.j. každý z pôvodcov informácie (prípadne každý zo správcov, majiteľov informácie) sa bude snažiť zvýšiť kvalitu ochrany, teda bude presadzovať väčší význam informácie, než táto ju v skutočnosti má.

Z hľadiska predmetu tohto výskumu je možné prehlásiť, že problém, ktorý riešime, sa nachádza práve v sektoroch A, B, C a D.

Keďže ide o pomerne transparentné relácie, je možné urobiť záver:
1. Rozdiel medzi utajovanou skutočnosťou a citlivou informáciou je iba inštitucionálny.
2. Ujma spôsobená citlivou informáciou vždy vedie v konečnom dôsledku ku ujme pre Slovenskú republiku (v škále zvrchovanosť, územná celistvosť, obrana, bezpečnosť, hospodárstvo, obyvateľstvo, ekológia, ekonomika a pod.).
3. Utajovaná skutočnosť a citlivá informácia sa líšia iba vo význame, rozsahu a v časovom rozlíšení eskalácie krízovej situácie vedúcej v konečnom dôsledku ku ujme pre Slovenskú republiku rôzneho významu, rozsahu a času manifestácie.
4. Citlivú informáciu je možné považovať ako aktívum, ktorého bezpečnostný význam je možné zistiť štandardnou rizikovou analýzou, pričom sa skúma riziko, ktoré môže viesť až ku ujme pre Slovenskú republiku.

Preskúmajme situáciu v sektoroch A, B, C a D podľa obr. 1.

Veľkosť jednotlivých sektorov je daná:
1. Presnosťou inštitucionálne stanovených kritických hraníc (napr. zoznamy utajovaných skutočností, alebo vymenovanie dokumentácie, ktorá obsahuje citlivé informácie podľa Prílohy 1 a Prílohy 2 atómového zákona).
2. Časovo ohraničenými podmienkami na hĺbku ochrany t.j. na prísnosť pohľadu na obsah informácie (napr. informácie týkajúce sa kontroly do vykonania kontroly sú omnoho citlivejšie, než po vykonanej kontrole).
3. Aktuálnou citlivosťou danou históriou (napr. ak v minulosti bola nejaká informácia prezradená, dnes je jej citlivosť veľmi sporná).
4. Mierou straty ostražitosti v príslušnej oblasti ochrany citlivých informácií a pod.

Hľadáme odpoveď na otázku: „Do akej miery je rozumné „podozrievať“ príslušnú informáciu, že jej obsah má potenciál zapríčiniť udalosti s následkom definovanej ujmy?“

Odpovede na túto otázku sa dajú rozdeliť na dve skupiny, ktoré zároveň tvoria hranice intervalu posudzovania citlivosti:

1. Liberálny (až avanturistický - anarchistický) postoj podnecovaný nesprávnym chápaním úlohy rozvoja demokracie („Nič nie je tajné, všetko je res publica - public affair“).
2. Paranoidný, neobjektívne podozrievavý postoj so snahou utajiť čo možno najväčšie množstvo informácií.

Objektívne by sa mala miera citlivosti posudzovať ako funkcia, ktorá zahŕňa:

1. Veľkosť potenciálnej ujmy.
2. Schopnosti útočníka (vedomosti, motivácia, iné).
3. Vybavenie útočníka (veľkosť zdrojov, ktoré má útočník k dispozícii).
4. Správnosť odhadu okolností a podmienok konania útoku (modus operandi).

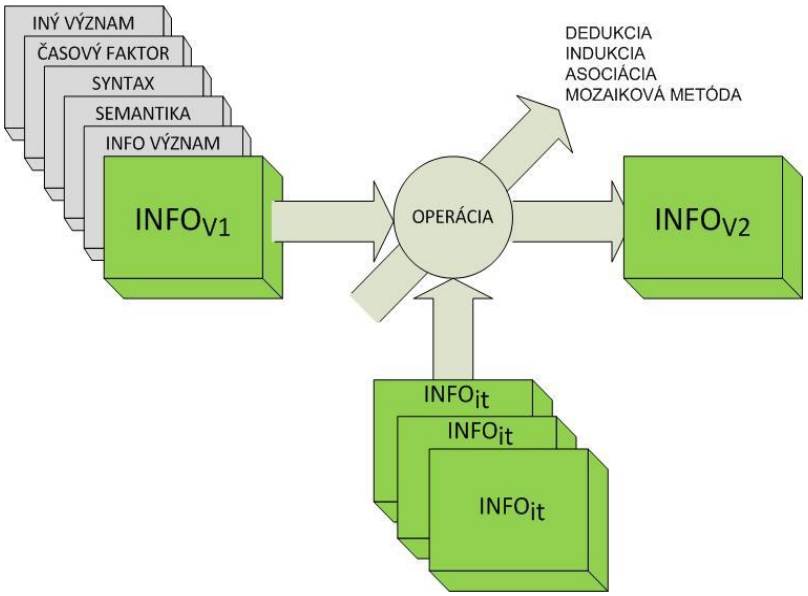
Miera citlivosti informácie priamo úmerne determinuje hĺbku ochrany príslušnej informácie.

Z uvedeného zatiaľ vyplýva, že „horná medza“ miery citlivosti je vymedzená zoznamom utajovaných skutočností.

Pásmo tolerancie je v právomoci pôvodcu informácie a v určitých prípadoch môže byť stanovené v pásme utajovaných skutočností. Dolná medza“ zostáva problémom. Predpokladáme, že odpoveď na otázku umiestnenia dolnej medze nájdeme vo výsledkoch analýzy rizík citlivých informácií.

3. MOŽNÁ DEFINÍCIA CITLIVEJ INFORMÁCIE

V tejto kapitole bude uvedená definícia citlivej informácie a popísané prístupy, pomocou ktorých bola táto pracovná hypotéza definície zostrojená.



Obrázok 2. **Transformácia informácie**

CITLIVÁ INFORMÁCIA je KAŽDÁ[01] informácia, na AKOMKOĽVEK[02] nosiči, v AKEJKOĽVEK[03] forme, s ktorou keď budeme MANIPULOVAŤ[04] (získanie, zneužitie, prezradenie, neúmyselné použitie, nevhodné použitie, a pod.), potom táto POSKYTNE[05], verifikuje, doplní a pod. inú informáciu, čo UMOŽNÍ INICIOVAŤ[06], alebo ZVÝŠIŤ RIZIKO[07], alebo eskaluje OHROZENIE[08], na základe ktorého táto skutočnosť môže pre HMOTNÉ AKTÍVUM[09], alebo PROCES[09], ktorá (ktorý) citlivú informáciu vlastní, alebo potrebuje pre svoje fungovanie, znamenať potenciálnu, alebo okamžitú UJMU[10] a táto informácia nie je utajovanou skutočnosťou v zmysle zákona o ochrane utajovaných skutočností (*definícia autora*).

Vysvetlenie indexov nad jednotlivými pojmami:

[01] Pojem vyjadruje, že akákoľvek informácia (napríklad podľa definície v nižšie

citovanom zákone o ochrane utajovaných skutočností, § 2 bod b), ktorá z hľadiska syntaxe, sémantiky, morfológie (v prenesenom slova zmysle to platí aj pre obrazovú a zvukovú informáciu) môže mať informačný obsah, ktorý je možné ďalej využiť na účely protiprávnej činnosti útočníka, v prípravnej, alebo realizačnej fáze. Ide hlavne o popis, nákres, videozáznam, videosekvencia (vytvorená umelými technikami), fotografia, mapa, audiozáznam a pod.

Príklad: Informácia uverejnená v spoločenskej rubrike merkantilného materiálu podniku „Ing. Ján NOVÁK, vedúci údržby v stredisku Riadiace systémy.“ Zdanlivo neúčinná informácia, ktorá ale môže byť využitá ako adresa pre útočníka pri hľadaní osoby, ktorá by sa dala vydierať, alebo inak zneužiť.

Aby sme nadbytočne nevyprodukovali vlastný pohľad na pojem „nosič“, pomôžeme si znením § 2 zákona č. 215/2004 Z. z.. Z uvedeného paragrafu vyplýva, že „nosič“, v ponímaní podstaty a určenia citlivej informácie, je hmotný objekt, ktorý dokáže informáciu uchovávať, prenášať, rozširovať a pod.

02 Opäť vystačíme so znením citovaného zákona o ochrane utajovaných skutočností, v § 2.

03 Rozmanitosť pojmu „manipulácia“ je značná. Ide o také operácie, alebo úkony s informáciou, ktoré sú úplne bežné v bežnom živote a zdanlivo nevytvárajú žiadne podozrenie na ohrozenie, nebezpečnosť týchto manipulácií a pod. Napr. majme dokument, v ktorom je potrebné začierniť citlivé informácie pred sprístupnením. Neobratnou elektronickou manipuláciou pri začierňovaní citlivých informácií, môže dôjsť ku stavu, že na začierňovanie sa použije reverzibilná počítačová operácia, ktorá dovolí útočníkovi rekonštrukciu informácie.

04 Obrázok 2 vyjadruje podstatu transformácie „verejnej“ (resp. zdanlivo verejnej) informácie na citlivú prostredníctvom operácií dedukcia, indukcia, asociácia, mozaiková metóda a pod. Pôvodná informácia, označená ako INFOV1 má viacero vrstiev, typov významov, vstupuje do interakcie z iným „verejnými“ (resp. zdanlivo verejnými) informáciami INFOit, ktorých môže byť nekonečné množstvo i a ktoré boli získané (prípadne spracované) v rôznom čase t. Takouto transformáciou vznikne informácia s významom 2 INFOV2.

05 Potenciál neoprávnene získanej citlivej informácie je závislý od schopností a možností útočníka. Vyťaženie obsahu danej informácie je možné vykonať interpretáciou ľudským intelektom, alebo pomocou algoritmov na analýzu a ďalšie spracovanie informácií, implementovaných vo výpočtových systémoch. Využitie takto získaného informačného obsahu je možné na prvotné oboznámenie sa, ale hlavne na doplnenie a/alebo verifikovanie predtým získanej informácie. Predpokladá sa, že hlavný spôsob využitie citlivých informácií je v tom, že dokážu doplniť a/alebo verifikovať – potvrdiť mozaiku obrazu určitej informačnej scény, ktorá má podstatne vyššiu mieru rizika ako samotná citlivá informácia.

06 V prípade, že citlivá informácia je svojim obsahom pôvodná (prvotne jedinečná), prebieha jej účinok na úrovni iniciácie určitého záujmu o túto informáciu u útočníka.

07 Ak je získaná informácia použitá na doplnenie mozaiky, spravidla jej účinok bude vo forme zvýšenia rizika.

08 Samotná informácia nemusí znamenať bezprostrednú manifestáciu ohrozenia, t.j. aktuálne pôsobenie rizika. Môže zvýšiť potenciál rizika, teda zvýšiť ohrozenie. V tejto súvislosti je dôležitá ďalšia forma pôsobenia citlivej informácie a to takmer časovo neobmedzené skryté pôsobenie informácií, ktoré boli kompromitované v minulosti a v súčasnej dobe sa tejto skutočnosti už nevenuje žiadna pozornosť.

09 Pojmy vyjadrujú skutočnosť, že citlivá informácia môže ohroziť nie len priamo, ale aj nepriamo. Myslí sa tým tá skutočnosť, že ohrozenie jadrového zariadenia nemusí mať iba „materiálu“ podobu, ale ide aj napr. o ohrozenie dobrého mena organizácie prevádzkujúcej určité zariadenia únikom citlivej informácie.

10 Ujma, ktorú citlivá informácia môže spôsobiť, je predmetom rizikovej analýzy. Pri analýze rizík bude citlivá informácia pôsobiť ako aktívum, ktoré je schopné iniciovať, alebo inak vplývať na odhalenie informácií inak dôverných s podstatne vyšším rizikovým potenciálom.

ZÁVER

1. Citlivé informácie sú informácie, ktoré, v rôznej miere, obsahujú skryté, nezjavné významy, súčasti informácií inak „obyčajne“ pôsobiacich, ktoré iniciujú pozornosť, dopĺňajú mozaiku, spresňujú, alebo potvrdzujú domnienku a znižujú neurčitosť.

2. Citlivá informácia je často katalyzátorom, na základe pôsobenia ktorého sa mení neurčitosť iných informácií, čo nakoniec vedie ku získaniu integrálnej informácie, ktorej dopadom môže byť ujma.
3. Ujma spôsobená citlivou informáciou je miera kvality iniciácie, doplnenia, spresnenia, zníženia neurčitosti inej informácie.
4. Hĺbka ochrany je funkciou schopnosti a možností útočníka.

LITERATÚRA

[1] SIVÁK, J. a kol.: *Záverečná správa z analýzy možných zdrojov úniku citlivých informácií o jadrových zariadeniach, vo vzťahu ku fyzickej ochrane jadrových zariadení*. Úrad jadrového dozoru Slovenskej republiky. Bratislava 2013.
[2] Zákon č. 143/2013, 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 a ktorým sa mení a dopĺňa zákon č. 238/2006 Z. z. o Národnom jadrovom fonde na vyraďovanie jadrových zariadení a na nakladanie s vyhoretým jadrovým palivom a rádioaktívnymi odpadmi (zákon o jadrovom fonde) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
[3] Zákon č. 45/2011 Z. z. o kritickej infraštruktúre.
[4] Metodické usmernenie Ministerstva hospodárstva Slovenskej republiky č. 1321/2011-1020 o ochrane citlivých informácií o kritickej infraštruktúre a o spôsobe manipulácie s týmito informáciami. (http://www.economy.gov.sk/metodicke-usmernenie-c-1321- 2011/137552s, získané 7.11.2013).
[5] Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.