# BEZPEČNOSŤ A KLASIFIKÁCIA ÚDAJOV V GEOGRAFICKÝCH INFORMAČNÝCH SYSTÉMOCH

**Mgr. Viera Gubková,**

Lynx spol. s r.o.

**Abstrakt:**

Bezpečnosť informačných systémov je založená na technických ale aj ľudských aspektoch. Jedným zo základných určujúcich aspektov pri výbere technických opatrení je presná a jednoznačná klasifikácia údajov v informačných systémoch. S klasifikáciou údajov priamo súvisí výber osôb a vymedzenie ich oprávnení pre prácu v informačnom systéme.

Pri budovaní bezpečnosti a tvorbe bezpečnostných projektov sa často dodávateľské komerčné firmy, ale aj samotný prevádzkovatelia informačných systémov (ďalej len IS), zaoberajú návrhom a realizáciou technických opatrení. Tieto doplnia rôznymi organizačnými opatreniami, zvolia diferencovaný prístup k údajom, ale k dôslednej klasifikácii sa nedostanú. Čo má za následok, že ľudský faktor, ktorý je najzraniteľnejšou časťou každého IS, zlyháva a stanovuje si vlastné pravidlá, ktoré sú v rozpore nielen so samotným bezpečnostným projektom, ale aj v rozpore s legislatívou SR. Podieľala som sa na výkone viacerých analýz rizík IS v štátnej správe i v komerčných organizáciách. Predmetom bola nielen ochrana utajovaných skutočností, ale aj bezpečnosť celej organizácie. Veľká časť mojich zistení sa dá zhrnúť pod jediný faktor: neznalosť. Neznalosť je veľmi často spôsobovaná neochotou samostatne sa vzdelávať a samostatne myslieť. Neochota sa odôvodňuje nedostatkom času, nedostatkom vnútorných predpisov a pod.. Podstata problému je však často v ľuďoch samotných, ktorí uprednostňujú „zvykové právo“ pred čímkoľvek novým, v nesprávnom využívaní pracovnej doby, v neustálom hľadaní odôvodnení a výhovoriek, prečo niečo nie je možné.

Oblasť personálnej a administratívnej bezpečnosti ovplyvňuje aj ohodnotenie zamestnanca. S primeraným ohodnotením stúpa zamestnancovi jeho sebavedomie, môže nadobudnúť pocit hrdosti na prácu, za ktorú je ohodnotený a zároveň stúpa profesná hrdosť. Aj zdanlivo nepodstatná vec ako je klasifikácia údajov a ohodnotenie zodpovednosti v popise pracovnej funkcie či náplne, môže viesť k zvýšeniu osobného ohodnotenia. Zatiaľ je to skôr výnimka. Vieme, že ak niekto pracuje s lopatou, má za ňu ohodnotenú hmotnú zodpovednosť, ale práca s informáciami, ktoré majú mnohomiliónové hodnoty, žiaľ, ohodnotená nie je.

Ďalším veľmi závažným rizikovým faktorom a jedným z najčastejších problémov u zákazníkov, je klasifikácia údajov. V jednom IS sa súčasne nachádzajú údaje, ktoré sú:

- verejne prístupné,
- predmetom obchodného tajomstva,
- osobné údaje,
- utajovanými skutočnosťami.

Neznalosť a nesprávna klasifikácia potom vedie k nesprávne stanoveným podmienkam prístupu, nevhodnému výberu osôb, nesprávne navrhnutým bezpečnostným opatreniam a v konečnom dôsledku k narušeniu dôvernosti údajov a bezpečnosti IS.

Pre každú z vyššie uvedených kategórií údajov platia iné legislatívne predpisy. Informácie môžu byť verejne prístupné v zmysle:

- zákona NR SR č. 211/2000 Z.z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií)
- zákona NR SR č.162/1995 Z.z. o katastri nehnuteľností a o zápise vlastníckych a iných práv k nehnuteľnostiam (katastrálny zákon).

Chránené obchodným tajomstvom v zmysle § 17 Obchodného zákonníka - zákona SNR č. 513/1991 Zb. Obchodné tajomstvo tvoria všetky skutočnosti obchodnej, výrobnej alebo technickej povahy súvisiace s podnikom, ktoré majú skutočnú alebo aspoň potenciálnu materiálnu alebo nemateriálnu hodnotu, nie sú v príslušných obchodných kruhoch bežne dostupné, majú byť podľa vôle podnikateľa utajené a podnikateľ zodpovedajúcim spôsobom ich utajenie zabezpečuje.

Narábanie s osobnými údajmi vymedzuje zákon o ochrane osobných údajov.

Podmienky na ochranu utajovaných skutočností, práva a povinnosti s tým súvisiace upravuje Zákon NR SR č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. V zmysle zákona vydal NBÚ viacero vyhlášok.

Utajovanou skutočnosťou je informácia alebo vec uvedená v zozname utajovaných skutočností, ktorú vzhľadom na záujem Slovenskej republiky treba chrániť pred vyzradením, zneužitím, poškodením, zničením, stratou alebo odcudzením.

Informáciou je

1. obsah písomnosti, nákresu, výkresu, mapy, fotografie, grafu alebo iného záznamu,
2. obsah ústneho vyjadrenia,

3. obsah elektrického, elektromagnetického, elektronického alebo iného fyzikálneho transportného média.

Vecou je

1. hmotný nosič so záznamom informácií,
2. výrobok,
3. zariadenie,
4. nehnuteľnosť.

Ujmou je také ohrozenie alebo poškodenie záujmov Slovenskej republiky alebo záujmu, ku ktorého ochrane sa Slovenská republika zaviazala, ktorého následky nemožno odstrániť alebo možno ich zmierniť iba následným opatrením; podľa významu záujmu a závažnosti spôsobenej ujmy sa ujma člení na mimoriadne vážnu ujmu, vážnu ujmu, jednoduchú ujmu a nevýhodnosť pre záujmy Slovenskej republiky.

Pôvodcom utajovanej skutočnosti je osoba, ktorá je oprávnená rozhodnúť, že informácia alebo vec je utajovanou skutočnosťou, určiť stupeň utajenia a rozhodnúť o zmene alebo zrušení stupňa jej utajenia.

Oprávnenou osobou je osoba, ktorá je určená na oboznamovanie sa s utajovanými skutočnosťami alebo ktorej oprávnenie na oboznamovanie sa s utajovanými skutočnosťami vzniklo zo zákona.

Nepovolanou osobou je osoba, ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami alebo ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami nad rozsah, ktorý jej je určený.

Technickým prostriedkom je zariadenie alebo systém určený na vytváranie, spracúvanie, prenos, ukladanie a ochranu utajovaných skutočností.

Utajované skutočnosti sa podľa stupňa utajenia členia na

a) prísne tajné,
b) tajné,
c) dôverné,
d) vyhradené.

V praxi znamená ochrana utajovaných skutočností vytváranie podmienok na personálnu, fyzickú, administratívnu, objektovú a priemyselnú bezpečnosť, šifrovú ochranu informácií a bezpečnosť technických prostriedkov.

Úmyselne som uviedla vymedzenie pojmov zo zákona a z www-stránky NBÚ. Vytváranie podmienok na ochranu utajovaných skutočností je rozdielne podľa stupňa

utajenia. Ak teda nesprávne klasifikujeme informácie a označíme ich iným stupňom utajenia aký určil pôvodca, môže sa stať, čo sa aj stáva, že porušíme zákon hneď niekoľkokrát.

Zo zoznamu utajovaných skutočností, ktorý tvorí vyhlášku NBÚ č. 432/2001 Z.z., prílohy č. 11 citujem niektoré utajované skutočnosti s uvedením stupňa utajenia:

25. Katalógy (zoznamy) údajov o trigonometrických bodoch zariadení na obranu štátu a ostatných účelových zariadení v súradnicovom systéme 1942 - PT

26. Katalógy súradníc geodetických bodov v systéme S-42/83 vrátane prílohových máp vydávané Topografickou službou armády a súradnice trigonometrických bodov zo súvislého územia väčšieho ako územie zobrazené v jednom mapovom liste mierky 1:100 000 - PT

109. Letecké a pozemné meračské snímky a snímky leteckého diaľkového prieskumu územia štátu, ak to ich povaha vyžaduje - T

111. Mapové podklady so zákresmy vojenských objektov vrátane ich ochranných a bezpečnostných pásiem na účely ochrany záujmov rezortu obrany - D,T

275. Mapové podklady, údaje o vojenskej stavebnej činnosti a konkrétnom využití, evidencia pohybu osôb a techniky týkajúca sa území na zabezpečenie obranyschopnosti štátu - D

276. Špeciálne mapy všetkých druhov a mierok v grafickej alebo digitálnej forme a databázy o území štátu - D

277. Topografické mapy so špeciálnou vojenskou nadstavbou, písomné a grafické pomôcky určené na operačnú prípravu územia, zoznamy, registre, databázy a ďalšie informácie v analógovej i digitálnej forme, ktoré sú určené pre potreby obrany štátu - D

278. Vojensko-geografické vyhodnotenia územia štátu - D

301. Údaje, mapové podklady a doklady slúžiace na vypracovanie priebežných ročných a záverečných správ o sanačných prácach na územiach určených na zabezpečenie obranyschopnosti štátu a vo vojenských objektoch - V

Z vybranej časti zoznamu je zrejmé, že zaradenie niektorých údajov správne podľa stupňa utajenia nie je vždy jednoznačné.

Vo svojej praxi som sa stretla s tým, že oprávnená osoba označovala výstupy z GIS poskytované stavebnej firme ako podklady pre stavbu inžinierskych sietí s označením „Tajné“. Čoho sa dopustila:

1. označila informáciu stupňom utajenia, ktorý jej neprináleží (nejednalo sa o „Katalóg“),

2. odovzdala utajovanú skutočnosť bez toho, aby si overila, či osoba, ktorej poskytuje utajovanú skutočnosť, má zodpovedajúce oprávnenie, čiže sama porušila zákon.

Na moju otázku, prečo tak konala, som dostala odpoveď: „Vždy im poskytujeme tieto informácie, lebo musíme, inakšie by nemohli stavať. Označenie „tajné“ má ten účinok, že sa budú lepšie starať o dôvernosť“. Základným problémom bol fakt, že daná osoba vyhlásila, že súradnice uvedené na výkrese sú súhrnnými údajmi resp. informáciami.

V zmysle terajšej legislatívy môže označiť stupňom utajenia len pôvodca informácie, nie ktorýkoľvek užívateľ podľa svojho uváženia. Teda podstata je v tom, že je potrebné pre každý IS zaviesť presnú klasifikáciu dát (informácií). Ak je problémom vymedziť kedy súradnice predstavujú súhrnné údaje (katalóg), potom musí o odovzdávaní príslušných výstupov rozhodovať len jediná osoba s náležitým vzdelaním a oprávnením. Postúpenie utajovaných skutočností zo štátneho orgánu právnickým osobám podlieha zvýšeným požiadavkám na zabezpečenie ich ochrany:

- možno postúpiť len tú utajovanú skutočnosť, ktorá je v pôsobnosti tohto štátneho orgánu,
- právnická osoba musí spĺňať podmienky priemyselnej bezpečnosti,
- postúpenie môže byť vykonané len na základe zmluvy, ktorá musí obsahovať zoznam osôb, rozsah ich oprávnenia na oboznamovanie sa s utajovanými skutočnosťami u právnickej osoby atď.,
- postúpenie sa môže vykonať až po súhlase ústredného orgánu štátnej správy, do ktorého pôsobnosti utajovaná skutočnosť patrí.

V súčasných podmienkach získanie priemyselnej bezpečnosti a bezpečnostné previerky osôb sú veľmi zdĺhavým procesom. Ak by sme označovali zo zvyku niektoré súhrnné grafické informácie ako utajované skutočnosti, mohlo by to viesť k značným škodám a zbytočným problémom.

Ak je potrebné postupovanú informáciu chrániť a nie je utajovanou skutočnosťou, môžeme využiť „fenomém“ obchodného tajomstva. V tomto prípade podmienky určuje právnická osoba, ktorá je „vlastníkom“ informácie. Zákon nevylučuje zavedenie tohto pojmu aj pre štátne orgány, inštitúcie, rozpočtové a iné organizácie.

Ešte stále pretrváva zvyk označovať vybrané citlivejšie informácie a dokumenty termínom „dôverné“. Predovšetkým v štátnych inštitúciách môže nastať situácia, že sa

utajované skutočnosti a tieto informácie, ktoré nie sú utajovanými budú označovať rovnakým termínom, čo predstavuje z hľadiska zabezpečenia ochrany utajovaných skutočností problém.

Ak som sa doposiaľ venovala predovšetkým poskytovaniu informácií smerom von, potom je potrebné aspoň príkladom naznačiť riziká, ktoré hrozia pri požadovaní informácií.

Príklad: inštitúcia požaduje od akciovej spoločnosti určité informácie v digitálnej forme z jej GIS. Ak táto inštitúcia, i keď štátna, nemá nárok zo zákona a požaduje informácie, musí počítať s tým, že jej požiadavka bude odmietnutá. Dôvody môžu byť rôzne:

- v GISe sa nachádzajú utajované skutočnosti, ktoré nevedia jednoducho oddeliť a technicky by po ich vyčlenení súbor stratil vypovedaciu schopnosť,
- v GISe sa nachádzajú informácie, ktoré sú predmetom obchodného tajomstva,
- do vybudovania GISu boli vložené značné prostriedky a stanovenie ceny by bol problém, resp. by mohla byť pomerne vysoká,
- akciová spoločnosť nemá záujem poskytovať informácie.

Často si ani tvorcovia máp neuvedomujú, že zobrazili objekty, ktoré sa stali objektmi s rôznou úrovňou dôležitosti a to napr. z pohľadu štátnych hmotných rezerv, alebo aj z pohľadu požiadaviek obrany štátu. Preto je potrebné všetky výstupy z GIS sledovať aj z pohľadu zmien kategorizácie údajov. Kategorizácia je proces, ktorý je živý, môže sa meniť v čase i legislatíve.

Okrem všeobecne záväzných právnych predpisov majú vplyv na návrh bezpečnosti aj normy, ktoré sa pri tvorbe bezpečnostných dokumentov využívajú. V apríli r. 2002 boli do sústavy STN zavedené aj normy z oblasti riadenia informačnej bezpečnosti. V norme Informačné technológie Kódex praxe manažérstva informačnej bezpečnosti – STN ISO/IEC 17799 je jednou zo základných požiadaviek klasifikácia údajov. Klasifikácia informácií je súčasťou kapitoly: Klasifikácia a riadenia aktív, Klasifikácia informácií. Jej cieľom je zabezpečiť pre informačné aktíva vhodnú úroveň ochrany. Informácie by mali byť klasifikované tak, aby na jej základe mohla byť označená potreba, priorita a stupeň ochrany. Pre každú klasifikáciu by mali byť definované procedúry narábania, ktoré by pokrývali všetky činnosti v rámci narábania s informáciami. Norma Informačné technológie Návod na manažérstvo bezpečnosti IT Časť 3: Techniky pre manažment bezpečnosti IT – STN ISO/IEC TR 13335 – 3 sa tiež zaoberá klasifikáciou informácií. Návrh bezpečnostných opatrení závisí aj od klasifikácie informačných aktív, ktoré je základom pre návrh bezpečnostných domén.

Bezpečnostné domény potom tvoria architektúru bezpečnosti IT, ktorá popisuje, ako môžu byť splnené požiadavky na bezpečnosť IT.

Samozrejme, že moja prednáška len naznačila problémy, ktoré môžu vzniknúť nevhodnou klasifikáciu informácií. Prednáška nebola školením z oblasti ochrany utajovaných skutočností, či práva, ani nevymedzila všetky možnosti klasifikácie údajov. Spôsob klasifikácie informácií je závislý od organizácie a od cieľa, ktorý chceme dosiahnuť. V závere by som si však dovolila upozorniť, že správna klasifikácia je podkladom a východiskom pre správne spracované bezpečnostné projekty.

**Použitá literatúra:**


1. Zákon NR SR č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov vrátane vykonávacích vyhlášok
2. Zákon č. 281/1997 Z. z. o vojenských obvodoch a zákon, ktorým sa mení zákon NR SR č. 222/1996 Z.z. o organizácii miestnej štátnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
3. Zákon č.162/1995 Z.z. o katastri nehnuteľností a o zápise vlastníckych a iných práv k nehnuteľnostiam (katastrálny zákon) v znení neskorších predpisov
4. Metodika pre tvorbu bezpečnostného zámeru, projektu a smernice v rezorte MO SR
5. Informačné technológie Návod na manažérstvo bezpečnosti IT Časť 1: Koncepcie a modely bezpečnosti IT – STN ISO/IEC TR 13335 – 1
6. Informačné technológie Návod na manažérstvo bezpečnosti IT Časť 2:Riadenie a plánovanie bezpečnosti IT – STN ISO/IEC TR 13335 – 2
7. Informačné technológie Návod na manažérstvo bezpečnosti IT Časť 3: Techniky pre manažment bezpečnosti IT – STN ISO/IEC TR 13335 – 3
8. Informačné technológie Návod na manažérstvo bezpečnosti IT Časť 4: Výber bezpečnostných opatrení – STN ISO/IEC TR 13335 – 4Informačné technológie Kódex praxe manažérstva informačnej bezpečnosti – STN ISO/IEC 17799