Bezpečnostné aspekty spracovania informácií

Klára Hennyeyová[1], Galina Gerhátová[2]
Slovenská poľnohospodárska univerzita v Nitre
Fakulta ekonomiky a manažmentu, Katedra informatiky
Tr. A. Hlinku 2,
Nitra, SR
e-mail[1, 2]: Klara.Hennyeyova@uniag.sk, Galina.Gerhatova@uniag.sk

Abstrakt
Informačná bezpečnosť je proces ochrany dát pred ich náhodným alebo úmyselným zneužitím osobami v rámci alebo mimo organizácie, vrátane zamestnancov, alebo aj obávaných hackerov. Narušenie bezpečnosti môže zahŕňať rôzne činnosti, napr. poškodenie vzhľadu webovej stránky, napadnutie počítačovým vírusom, zlyhanie zamestnanca, ktorý neúmyselne prezradí svoje heslo, a pod.
Informácia je aktívum, nevyhnutné pre činnosť organizácie a teda rovnako ako pri iných aktívach je potrebné zabezpečiť jeho ochranu, primeranú jeho významu a cene, akú má pre organizáciu. Informácia môže byť verbálna, písaná alebo vytlačená na papieri alebo uložená v elektronickej forme.
Klasický model informačnej bezpečnosti sa zameriava na 4 hlavné oblasti zabezpečenia ochrany dát:
- *Technická bezpečnosť – ochrana uchovávaných dát pred stratou v dôsledku zlyhania niektorej časti informačného systému.*
- *Sieťová bezpečnosť – ochrana dát pred ich stratou, respektíve odcudzením pomocou sieťového pripojenie – internetu.*
- *Ľudský faktor – ochrana dát pred stratou v dôsledku neodborného zaobchádzania, či inými hrozbami spôsobenými zamestnancami.*
- *Podnikateľský faktor – analýza efektivity procesov súvisiacich s informačnými systémami a ich optimalizácia s cieľom zvyšovania konkurencieschopnosti.*

Hlavnou úlohou v oblasti informačnej bezpečnosti je vytvoriť jednotnú platformu budovania informačnej spoločnosti postavenú na právnych základoch so zabezpečením primeranej ochrany a dôveryhodnosti digitálneho priestoru. V mnohých podnikoch sa informačnej bezpečnosti stále nevenuje dostatočná pozornosť. Je to spôsobené jednak neznalosťou problematiky informačnej bezpečnosti a nedocenením hrozieb a rizík, ale aj zlou ekonomickou situáciou podnikov, v dôsledku čoho nie sú vyčlenené finančné zdroje na zabezpečenie ochrany informačných systémov a informačných technológií. V podnikoch by mala byť vypracovaná bezpečnostná politika a smernice na jej dodržiavanie.

Kľúčové slová: *informačná bezpečnosť, informácia, informačný systém, IKT, bezpečnostná politika*

JEL klasifikácia: *L86*

1. Úvod

Dostupnosť správnych informácií, v správnom čase a potrebnej forme sa stáva čoraz väčšou nevyhnutnosťou vo väčšine priemyselných odvetví, v službách i vo verejnej správe. Manipulácia s obrovským množstvom informácií, často dôverného charakteru, prináša so sebou i nesmierne riziká ich úniku, straty alebo zneužitia.

Informačná bezpečnosť je ochrana informácií pred hrozbami a zraniteľnosťami s cieľom zabezpečiť kontinuálny a úspešný chod činností organizácie, minimalizovať podnikateľské riziko a maximalizovať využitie investícií a obchodných príležitostí.

V súvislosti s pojmom bezpečnosť informácií je nutné sa zmieniť ešte o ďalších dvoch pojmoch, a to bezpečnosť organizácie a bezpečnosť informačných systémov (IS) a informačných technológií (IT).

Najvyššia kategória je bezpečnosť organizácie. Jej súčasťou je zaistenie bezpečnosti objektov, majetku organizácie, ako je ochrana prístupov do objektov, strážna služba a pod. Niektoré jej

činnosti napomáhajú zároveň i zaistenie bezpečnosti IS a IT (napr. kontrola oprávnenia fyzického prístupu do budov). Jej súčasťou okrem iného je aj bezpečnosť informácií. Cieľom a úlohou riadenia bezpečnosti informácií je zhrnúť v sebe zásady bezpečnej práce s informáciami všetkého druhu, teda nielen s informáciami v digitálnej forme. Bezpečnosť informácií zahŕňa tiež spôsob spracovania dát, ich uloženie a správy archívov nedigitálnych dát, zásady skartácie materiálov, nakladanie s informáciami v priebehu ich transportu na iné miesta, zásady pre poskytovanie informácií novinárom, zásady pre verejné vystupovanie pracovníkov organizácie napr. v rozhlase alebo televízii a pod.

Ochranu informácií môžeme dosiahnuť implementáciou opatrení ako sú politiky, procesy, postupy, organizačné štruktúry a softvérové a hardvérové funkcie. Tieto opatrenia je nutné implementovať, monitorovať, analyzovať a zlepšovať všade tam, kde je to potrebné na splnenie špecifických bezpečnostných a podnikateľských zámerov organizácie.

2. Dáta a metodológia

Informačná bezpečnosť predstavuje vytvorenie bezpečného informačného systému (IS), v ktorom je zaistená ochrana údajov, ktoré IS spracováva a uchováva tak, aby nedochádzalo k úniku informácií neoprávneným osobám.

Podľa definície medzinárodného štandardu ISO/IEC 27001 [9], informačná bezpečnosť zahŕňa a poskytuje 3 hlavné atribúty: dôvernosť, integritu a dostupnosť (známu ako CIA).

Z hľadiska ochrany údajov môžu vzniknúť nasledujúce útoky proti týmto atribútom spracovávaných údajov v IS:

a) Porušenie alebo strata ***dôvernosti*** údajov.
   Dôvernosť (**C**onfidentiality) – údaje nie sú sprístupňované a odhaľované neautorizovaným osobám, entitám, alebo procesom.
   Dôvernosť je atribút údaja, ktorý zabezpečuje, že údaj nebude poskytnutý, odhalený alebo zneužitý neoprávneným subjektom. Dôvernosť predstavuje hierarchicky usporiadaný mechanizmus, ktorý zaručí požadovaný stupeň oprávnenia na zápis a čítanie údajov v určenej časti zabezpečovacieho systému. Porušenie dôvernosti môže spôsobiť, že údaje z IS budú prístupné neautorizovaným jednotlivcom alebo procesom.
b) Porušenie alebo strata ***integrity*** údajov.
   Integrita (**I**ntegrity) – zabezpečenie presnosti a úplnosti aktív.
   Integrita reprezentuje neporušiteľnosť vložených údajov zásahom technickej časti systému alebo ľudského činiteľa. Rozlišujeme *integritu údajov* (ochrana údajov pred zmenou alebo zničením neautorizovaných spôsobom) a *integritu systému* (ochrana informačného systému ako celku s cieľom nerušenej práce s údajmi bez náhodnej neautorizovanej manipulácie so systémom). Porušenie integrity znamená neautorizovaný príjem, neautorizované vyslanie alebo neautorizovanú transformáciu údajov.
c) Strata ***dostupnosti*** údajov.
   Dostupnosť (**A**vailability) – schopnosť byť dostupný a použiteľný na požiadanie autorizovanej entity.
   Dostupnosť je časová charakteristika, ktorá vyjadruje závislosť medzi požiadavkami riadeného systému a splnením týchto požiadaviek. Vyjadruje sa pravdepodobnosťou oneskorenia medzi žiadosťou o službu a jej realizáciou. Strata dostupnosti môže znamenať nesplnenie požiadavky systému, resp. neprístupnosť a nepoužiteľnosť údajov autorizovaným jednotlivcom alebo procesom v požadovanom čase.

Cieľom príspevku je definovať základné atribúty bezpečného využívania informačných a komunikačných technológií a informačných systémov v podnikoch a navrhnúť postupy budovania bezpečnostnej politiky podniku.

Pri spracovaní príspevku sme vychádzali z výsledkov dotazníkového prieskumu zameraného na informačnú bezpečnosť v podnikoch, ktorý sme realizovali v rámci výskumu na Katedre informatiky FEM SPU v Nitre, ako aj z osobných skúseností a poznatkov z predmetnej problematiky.

3. Výsledky a diskusia

3.1 Bezpečnosť informačných systémov a ochrana údajov

Informačný systém sa skladá z určitého množstva komponentov (aktív), ktoré spolu tvoria ucelený systém, ktorý je potrebné adekvátnym a efektívnym spôsobom chrániť tak, aby sa dosiahol stav tzv. „zdravého“ informačného systému. Od spoľahlivej prevádzky IS často závisí schopnosť jeho užívateľov vykonávať svoju predpokladanú činnosť, plniť svoje záväzky voči ďalším subjektom, ako aj včas prijímať správne rozhodnutia. Zabezpečenie spoľahlivej prevádzky IS znamená uskutočnenie takých bezpečnostných opatrení, ktoré umožnia informačnému systému plniť úlohy a funkcie, pre ktoré bol vybudovaný, poskytovať svoje služby užívateľom včas a v požadovanej kvalite.

Údaje, ktoré sa spracovávajú v IS majú svoje vlastnosti – atribúty, ako napr. presnosť, správnosť, úplnosť, vierohodnosť, relevantnosť a pod. Ochrana údajov v IS musí byť zameraná na opatrenia na zachovanie takých atribútov spracovávaných údajov, ktoré sú užívateľom považované za dôležité. Pri formulovaní požiadaviek na zabezpečenie ochrany údajov je veľmi dôležité správne určiť, ktoré údaje a ktoré atribúty údajov konkrétneho systému je potrebné chrániť a na akej úrovni.

Na zníženie pôsobenia hrozieb na konkrétne aktíva je potrebné definovať *ochranné opatrenia.* Sú to praktiky, postupy alebo mechanizmy, ktoré môžu poskytnúť ochranu pred hrozbou, znížiť zraniteľnosť, obmedziť dopad nežiaduceho incidentu, detekovať nežiaduci incident a uľahčiť obnovu integrity IS.

Účinná bezpečnosť zvyčajne vyžaduje kombináciu rôznych ochranných opatrení, aby poskytovala aktívam adekvátny stupeň bezpečnosti. Ochranné opatrenia sú nástrojom na znižovanie veľkosti výsledného rizika. Cieľom konkrétnych bezpečnostných ochranných opatrení je eliminovať pôsobenie hrozieb na konkrétne aktíva informačného systému. Je to teda zvládanie rizík. Ochranné opatrenia môžu riziká, pôsobiace na informačný systém akceptovať, znížiť, maximálne eliminovať alebo len presunúť na iné miesto.

Ochranné opatrenia členíme na:
- *opatrenia v oblasti fyzickej bezpečnosti* (protipožiarna ochrana, ochrana pred vodou a prírodnými katastrofami, ochrana pred krádežou, ochrana elektrického napájania a klimatizácie a pod.)
- *opatrenia v oblasti informačnej bezpečnosti* (firewall, antivírusová ochrana, ochrana údajov prenášaných prostredníctvom siete, ochrana logického prístupu k údajom a pod.)
- *režimové a organizačné opatrenia* (vnútropodnikové bezpečnostné smernice v oblasti fyzickej aj informačnej bezpečnosti, školenia zamestnancov v oblasti využívania IT a informačnej bezpečnosti, vytváranie bezpečnostného povedomia a pod.)

3.2 Bezpečnostná politika a bezpečnostný projekt

Bezpečnostnú politiku informačného systému nie je možné budovať samostatne, ale z dôvodu komplexnosti a nadväznosti je potrebné, aby vychádzala z celkovej bezpečnostnej politiky podniku a nadväzovala na súhrn ochranných opatrení vypracovaných v rámci Ochrany majetku, Bezpečnosti a ochrany zdravia pri práci, Požiarnej bezpečnosti a pod.

Bezpečnostná politika podniku je základný písomný dokument podniku, ktorý obsahuje predstavu vedenia o riešení bezpečnosti a vymedzenie základných požiadaviek na jednotlivé oblasti celého informačného systému. Ak podnik prevádzkuje IS, súčasťou bezpečnostnej politiky podniku by mala byť bezpečnosť IS a jeho súčastí, bezpečnosť prenosu, spracovávania a uchovávania informácií a vymedzenie zodpovednosti za jednotlivé oblasti. Bezpečnostná politika je v praxi chápaná ako základné východisko pre riadenie bezpečnosti IS. Vyjadruje bezpečnostné ciele, definuje zásady procesu ochrany, všetky pravidlá, postupy a obmedzenia, ktoré určujú spôsob správy, ochrany a distribúcie citlivých informácií z IS. Cieľom bezpečnostnej politiky je minimalizovať vplyv pôsobiacich rizík v zmysle vypracovaných všeobecných pravidiel a postupov pre konkrétny informačný systém.

Bezpečnostná politika predstavuje súhrn ochranných opatrení pre riešenie informačnej bezpečnosti na úrovni fyzickej, komunikačnej, počítačovej, logickej a personálnej. Úlohou bezpečnostnej politiky je definovať jednotlivé hrozby, ktoré sú relevantné pre aktíva IS a popísať ochranné opatrenia na elimináciu týchto hrozieb.

Bezpečnostná politika ponúka odpovede na niekoľko základných otázok:
- Čo chceme chrániť.
- Prečo to chceme chrániť.
- Ako to chceme chrániť.
- Čo budeme robiť, keď dôjde k zlyhaniu systému.

Bezpečnostná politika je písomný dokument, ktorý musí byť schválený vedením podniku ako záväzná vnútropodniková smernica. Jeho hlavnou úlohou je určiť zamestnancom základné pravidlá pri používaní informačných zdrojov, ako aj vysvetliť, čo je považované za povolené a čo nie. Mala by zahŕňať všetky komponenty IS, ktorými sú hardvér, softvér, údaje a používatelia. Dobre navrhnutá bezpečnostná politika je kompromisom v obmedzovaní užívateľov a chráneným záujmom organizácie. Dobre vybudovaná bezpečnostná politika je základom pre úspešnú implementáciu budúcich projektov zameraných na bezpečnosť IS.

Bezpečnostný projekt rieši vhodný spôsob zabezpečenia ochrany s ohľadom na každý prvok systému, ako aj na systém ako celok. Zohľadňuje špecifické vlastnosti, určenie a druh chráneného informačného systému.

Cieľom bezpečnostného projektu je vymedziť rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti, funkčnosti a ochrany osobných údajov. Bezpečnostný projekt sa spracováva v súlade so základnými pravidlami bezpečnosti informačného systému vydanými bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami.

Bezpečnostný projekt by mal obsahovať nasledujúce časti: bezpečnostný zámer, analýzu rizík, plán implementácie ochranných opatrení, bezpečnostné smernice, havarijný plán a plán obnovy IS.

3.2.1 Bezpečnostný zámer

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti. Bezpečnostný zámer

posudzuje súčasný stav IS a jeho ochrany a špecifikuje problémy a nedostatky, vymedzuje kľúčové problémové oblasti, ktoré je nutné riešiť. Jeho hlavným cieľom je zaistenie integrity, dostupnosti, dôvernosti, spoľahlivosti, zodpovednosti a autenticity informačných systémov.

Bezpečnostný zámer obsahuje:
- formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,
- stanovenie predmetu ochrany,
- špecifikáciu technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia,
- stanovenie oprávnenia používania technických prostriedkov,
- vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti,
- definovanie požiadaviek na bezpečnosť,
- vymedzenie hraníc určujúcich množinu zvyškových rizík.

3.2.2 Analýza a riadenie rizík a návrh nových alebo doplňujúcich ochranných opatrení

Analýza bezpečnosti informačného systému je podrobný rozbor stavu bezpečnosti informačného systému, ktorá obsahuje najmä kvalitatívnu analýzu rizík. V rámci analýzy rizík sa identifikujú hrozby pôsobiace na jednotlivé aktíva informačného systému, ktoré môžu narušiť jeho bezpečnosť alebo funkčnosť. Výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov, s uvedením rozsahu možného rizika, návrhov opatrení, ktoré eliminujú alebo minimalizujú vplyv rizík. Súčasťou analýzy bezpečnosti informačného systému je aj posúdenie zhody navrhnutých bezpečnostných opatrení s platnými a používanými bezpečnostnými štandardmi, metódami a prostriedkami.

Riziko v informačných systémoch je charakterizované ako kombinácia troch bezpečnostných prvkov – *aktív, hrozieb* a *zraniteľnosti*.

Analýza rizík identifikuje hrozby a ich riziká, ktoré je potrebné akceptovať alebo korigovať. Riziká sú odhadované z hľadiska možného dopadu, spôsobeného narušením dôvernosti, integrity, dostupnosti atď.

Riadenie rizika je rozhodovací proces nadväzujúci na výsledky procesu hodnotenia rizík. Cieľom procesu riadenia rizík je navrhnutie optimálneho spôsobu zníženia rizika na spoločensky prijateľnú mieru rizika. Optimálny spôsob zohľadňuje ekonomické, sociálne, technické, politické i ďalšie faktory.

Riadenie rizika je kľúčovým nástrojom pre systematické riadenie bezpečnosti informácií. Presná znalosť skutočných rizík rozhoduje o výbere a presadzovaní vhodných bezpečnostných opatrení schopných znížiť negatívne dopady týchto rizík. Dobrá a presná znalosť bezpečnostných rizík vedie k účinnému vynakladaniu úsilia pri presadzovaní bezpečnostných opatrení, ktoré tak prinášajú väčšiu efektivitu. Riadenie rizík je preto základom pre každý systém riadenia bezpečnosti informácií a podstatným spôsobom ovplyvňuje efektivitu fungovania celého IS.

3.2.3 Plán implementácie nových alebo doplňujúcich ochranných opatrení

Definuje pravidlá a opatrenia, ktoré sa musia prijať, aby mohli byť navrhované ochranné opatrenia čo najúčinnejšie implementované v praxi.

Plán implementácie je zameraný na:
- určenie priority jednotlivých navrhovaných ochranných opatrení ,
- časový harmonogram implementácie vo vzťahu k prioritám,
- finančný rozpočet potrebný na implementáciu ochranných opatrení,

- zodpovednosť jednotlivých pracovníkov,
- prípravu školenia o bezpečnosti IS a vytvorenie povedomia o bezpečnosti medzi užívateľmi.

3.2.4 Bezpečnostné smernice

Stanovujú postupy a pravidlá pri používaní technických prostriedkov, užívateľské a administrátorské práva, organizačnú štruktúru, rozdelenie zodpovednosti a právomoci a celkový proces ochrany aktív.

K jednotlivých skupinám informačných aktív patria:
- *údaje a informácie*: informácie spracovávané v IS, databázy, archivované súbory, programová dokumentácia k IS a pod.,
- *softvér*: operačný systém, aplikačný softvér, informačný systém,
- *technické prostriedky*: počítače, tlačiarne, multimediálne zariadenie, externé disky, USB kľúče a pod.

Bezpečnostné smernice upresňujú a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovaného informačného systému a obsahujú najmä :
- opis informačného systému,
- typy a klasifikáciu chránených informácií,
- popis technických, organizačných a personálnych opatrení vymedzených v bezpečnostnom projekte a ich využitie v konkrétnych podmienkach,
- rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému,
- zásady manipulácie s chránenými informáciami,
- postupy a pravidlá pre zálohovanie a archiváciu,
- rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,
- spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,
- zásady antivírusovej ochrany a ochrany pred neoprávneným vstupom do IS,
- politiku tvorby a prideľovania hesiel,
- postupy likvidácie nepotrebných údajov,
- postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou.

3.2.5 Havarijný plán a plán obnovy IS

Havarijný plán určuje, čo sa má vykonať po odhalení bezpečnostného incidentu a ako postupovať, aby sa udržala kontinuita činnosti spoločnosti.

Havarijný plán určuje miesto a spôsob zálohovania údajov, postupy udržovania aktuálnosti skladov údajov, softvéru a hardvéru, spôsoby aktualizácie a testovania hardvéru.

Súčasťou havarijného plánu sú:
- plán činnosti po útoku – návod, ako postupovať v poskytovaní služieb po zistení bezpečnostného incidentu, dohody o poskytovaní náhradných riešení informaticky orientovaných úloh spoločnosti, a dohody o uvedení údajov IS do pôvodného stavu po havárii.
- plán obnovy – návod, ako postupovať pri obnove činnosti IS po havárii.

Spracovanie bezpečnostných incidentov je nákladné tak finančne ako aj časovo. Čas potrebný na detekciu útočníkov, určenie rozsahu škôd a následnú elimináciu bezpečnostných dier predstavuje nepredpokladané výdaje. Podľa oblasti pôsobenia podniku môže mať za následok

pokles dôvery v podnik, stratu klientov, stratu dobrého mena a v konečnom dôsledku pokles finančného profitu. Je vhodné, aby mal podnik vypracovaný krízový plán pre prípad riešenia bezpečnostného incidentu.

3.3 Odporúčania v oblasti informačnej bezpečnosti pre prax

Hlavnou úlohou v oblasti informačnej bezpečnosti je vytvoriť jednotnú platformu budovania informačnej spoločnosti postavenú na právnych základoch so zabezpečením primeranej ochrany a dôveryhodnosti digitálneho priestoru. V mnohých podnikoch sa informačnej bezpečnosti stále nevenuje dostatočná pozornosť. Je to spôsobené jednak neznalosťou problematiky informačnej bezpečnosti a nedocenením hrozieb a rizík, ale aj zlou ekonomickou situáciou podnikov, v dôsledku čoho nie sú vyčlenené finančné zdroje na zabezpečenie ochrany IS a IT.

Finančné prostriedky vynaložené v podnikoch na zlepšenie stavu informačnej bezpečnosti nemajú priamo vyčísliteľnú návratnosť. Implementácia bezpečnostných riešení však znižuje pravdepodobnosť vzniku bezpečnostných incidentov, ktoré takmer vždy znamenajú straty v dôsledku zneužitia informácií alebo znefunkčnenia informačného systému. V podnikoch by mala byť vypracovaná bezpečnostná politika a smernice na jej dodržiavanie. Pri budovaní bezpečnostnej politiky sa nedá postupovať náhodne a chaoticky, je nutné sa riadiť jasne definovanými postupmi. Tie je možné voľne popísať nasledovne: *stanovenie cieľov a stratégie riešenia informačnej bezpečnosti, definícia aktív, analýza rizík, tvorba bezpečnostnej politiky, stanovenie bezpečnostných štandardov, implementácia bezpečnosti, monitoring a audit*.

Na zlepšenie úrovne informačnej bezpečnosti v podniku je možné definovať nasledujúce odporúčania:
- Definovanie prístupových práv používateľov IT a IS.
- Definovanie zodpovednosti používateľov IT a IS za vznik a riešenie bezpečnostných incidentov.
- Klasifikácia informácií v podniku podľa citlivosti.
- Odhalenie a riešenie bezpečnostných incidentov.
- Vypracovanie bezpečnostných smerníc.
- Definovanie aktív v podniku.
- Vzdelávanie v oblasti bezpečného využívania IT a IS v podniku.

4. Záver

Bezpečnostná politika je základným a východiskovým dokumentom na projektovanie každého bezpečnostného systému. Predstavuje deklaráciu zodpovednosti subjektu bezpečnosti (organizácie, firmy a pod.) za bezpečnosť osôb, ochrany majetku a informácií. Bezpečnostná politika sa vypracúva spravidla po predchádzajúcej analýze bezpečnostných rizík.

Samotná bezpečnosť IS a IT má za úlohu chrániť aktíva, ktoré sú súčasťou informačného systému podniku. Základný koncept zaistenia bezpečnosti IS a IT predstavuje vzťahy medzi aktívami organizácie, hrozbami, ktoré na ne môžu potenciálne pôsobiť, možnou zraniteľnosťou aktív reálnymi hrozbami, dopady reálnych hrozieb na tieto aktíva a možnosťami ochrany aktív organizácie formou opatrení.

Pri zabezpečení ochrany údajov nesmieme zabúdať na potrebu chrániť prístupové heslá oprávnených užívateľov alebo šifrovacie kľúče, nakoľko neoprávnená manipulácia s takýmito údajmi môže mať za následok veľké škody spojené s únikom údajov a ich zneužitím.

Literatúra

[1] DEKÝŠ, P. (2010). Správa informačnej bezpečnosti v malej a stredne veľkej spoločnosti. Dostupné na: http://www.eset.com/sk/firmy/services/clanky/sprava-informacnej-bezpecnosti/.

[2] DOUCEK, P., NOVÁK, L. & SVATÁ, V. (2008). Řízení bezpečnosti informací. 1. vyd. Praha. Professional Publishing, 2008, s. 59-63, 98-105. ISBN 978-80-86946-88-7.

[3] GÁPA, M. (2006). Bezpečnosť informačných systémov : diplomová práca. Žilina : Žilinská univerzita, 2006, 105 s.

[4] HAMÁŠOVÁ, K. & HENNYEYOVÁ, K. (2012). Analýza rizika v skúmanom podniku agrosektora. In: Zborník príspevkov z MVD 2012 „Globálne komoditné trhy: Nové výzvy a úloha verejných politík". Nitra, 2012. s. 408-412. ISBN 978-80-552- 0792-6.

[5] HENNYEYOVÁ, K. & HAMÁŠOVÁ, K. (2012). Aspekty informačnej bezpečnosti v podnikoch agrosektora : vedecká monografia. Nitra : SPU, 2012. 123 s. ISBN 978-80-552-0879-4.

[6] HENNYEYOVÁ, K., KORCOVÁ, Z. & POPELKA, V. (2010). Selected aspects of the information security in Slovakia. In Global Economy 2010. (CD). Nitra : SPU, 2010 s. 2559-2565. ISBN 978-80-552-0386-7.

[7] Informačná bezpečnosť. (2011). [online], aktualizované 2015. Dostupné na: http://www.virte.sk/produkty-a-sluzby/informacna-bezpecnost/.

[8] Informačná bezpečnosť. (2012). [online], aktualizované 2015. Dostupné na: http://www.disig.sk/index.php?id=ismain&L=fpltjssunkto.

[9] ISO/IEC 27001. Informačná bezpečnosť – cenné aktívum. (2009). [online], aktualizované 2009. Dostupné na: http://www.vincotte.sk/component/content/article/32.html.

[10] Národná stratégia pre informačnú bezpečnosť SR. (2011). [online]. Ministerstvo financií Slovenskej republiky, aktualizované 2014. Dostupné na: http://www.informatizacia.sk/narodna-strategia-pre-ib/6783c.

[11] Smernice OECD za kultúru bezpečnosti. (2002). [online]. Ministerstvo financií Slovenskej republiky, aktualizované 2010. Dostupné na: http://www.informatizacia.sk/smernice-oecd/3001s.