[7] Gážiová,M.: Minimálne požiadavky na zariadenia a prostredie pracovísk so zobrazovacími jednotkami a na programové vybavenie, Bezpečnosť práce, 11/2003, str. 20-26
[8] Vyhláška Ministerstva zdravotníctva Slovenskej republiky č. 271/2004 Z. z. o ochrane zdravia pred neionizujúcim žiarením
[9] Göblová,G.: Minimalizácia rizík na vybraných pracoviskách s elektromagnetickým poľom, DP, KBaKP, SjF TU Košice, 2004
[10] Hamráková,L.: Posúdenie rizík v oblasti nízkofrekvenčných EMP v prevádzke strojárenského podniku, DP, KBaKP, SjF TU Košice, 2005

Komplexní bezpečnost IS

Doc. Ing. Milena Tvrdíková, CSc.
VŠB-TU Ostrava, EkF,
Katedra aplikované informatiky,
Sokolská tř.33., Ostrava 1, 701 00
e-mail: milena.tvrdikova@vsb.cz

Abstrakt

Bezpečnost informačního systému je důležitou součástí jeho koncepce a vývoje. Význam kvalitního zabezpečení informačních systémů stále roste. Bylo by však chybné zužovat tento problém pouze na problematiku ošetření bezpečnosti informačních technologií, neboť informační technologie jsou pouze jednou z částí informačních systémů. Je nezbytné nahlížet na jeho bezpečnost komplexně a snažit se o zabezpečení IS dané organizace ve všech jeho částech a na všech jeho rozhraních.

Příspěvek je snahou o ucelený pohled na bezpečnost IS. Hovoří o bezpečnosti informačních systémů z pohledu jeho jednotlivých složek – hardwaru, softwaru, peopleware, dat i vlivů reálného světa.

Klíčová slova

Bezpečnost IS, komponenty IS, informační technologie, uživatel, reálný svět, bezpečnostní politika

Komponenty IS

Bezpečnost informačního systému (dále IS) je důležitou součástí jeho koncepce a vývoje. Význam kvalitního zabezpečení IS stále roste. Bylo by však chybné zužovat tento problém pouze na problematiku ošetření bezpečnosti informačních technologií (dále IT), neboť IT jsou pouze jednou z částí IS. Je nezbytné nahlížet na bezpečnost IS komplexně a snažit se o zabezpečení IS dané organizace ve všech jeho částech a na všech jeho rozhraních.

Otázka zajištění komplexní bezpečnosti IS bývá často podceňována, protože pokud nedojde v IS k žádnému bezpečnostnímu incidentu nepřináší vložené investice žádné konkrétní výsledky.

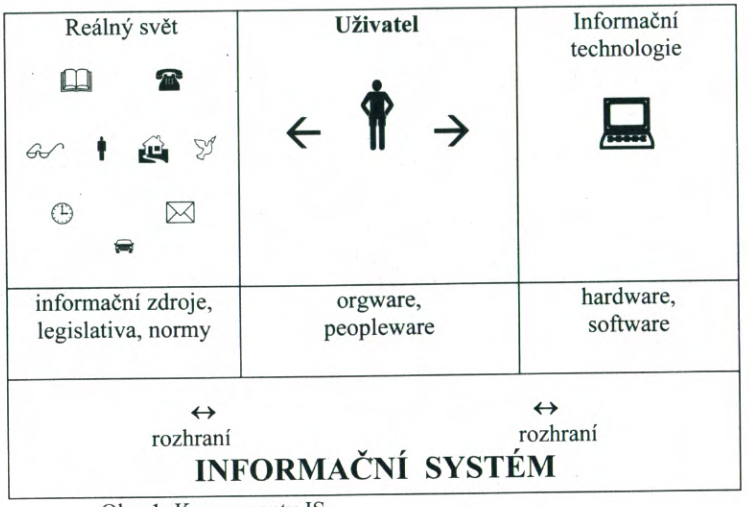
Z následujícího obrázku vyplývá, že IS je tvořen nejen IT, ale i jeho uživateli a okolním reálným světem, ve kterém funguje. Je tedy potřebné zabývat se bezpečností všech jeho komponent a také bezpečností vlastního bohatství IS, tj. uchovávaných, přenášených a zpracovávaných informací.

ÚTOKY NA INFORMAČNÍ TECHNOLOGIE

IT jsou tvořeny hardwarem, softwarem na jejichž rozhraní směrem k uživateli se pohybují data.

Útoky na IT lze dělit na:

- **přerušení** nebo **zničení** (dočasné nebo trvalé ukončení dostupnosti některé komponenty IS),
- **odposlech** – neautorizovaný přístup k některé komponentě IS,
- **změna** – modifikace některé z komponent IS,
- **přidání funkcí nebo dat** – průnik dezinformací do IS.



Obr. 1. Komponenty IS

Útokům na **hardware** lze většinou zabránit bezpečnostními systémy a důsledným střežením objektů. Jedná se tyto typy útoků:

- Přerušení nebo zničení – havárie (přírodní živly), poškození, krádež
- Odposlech – krádež (zařízení, procesoru, paměti nebo místa v paměti)
- Přidání funkcí – změna režimu činnosti.

Útoky na **software** jsou většinou dílem profesionálů a nelze jim zcela zamezit, lze však bezpečnostními opatřeními tuto činnost útočníkům ztížit.

- Přerušení nebo zničení – vymazání softwaru (úmyslné nebo neúmyslné)
- Odposlech – kopírování
- Změna – modifikace software
- Přidání funkcí nebo dat – chyby, viry apod.

Jednotlivými komponentami bezpečnosti dat jsou:

- **integrita** – zajištění, že data jsou přesná, očištěná a chráněná proti neautorizované změně,
- **důvěrnost** – zajištění prevence neautorizovaného vyzrazení v každém okamžiku zpracování dat,
- **dostupnost** – IS musí mít datovou kapacitu dimenzovanou tak, aby poskytoval spolehlivou a včasnou dispozici dat autorizovaným jednotlivcům.

Útoky na **data** (jsou velmi nebezpečné neboť data jsou často nenahraditelná, jsou interním bohatstvím každého informačního systému):

- Přerušení nebo zničení – vymazání dat (úmyslné nebo neúmyslné)
- Odposlech – kopírování dat
- Změna – modifikování dat
- Přidání hodnoty – modifikace transakcí.

OCHRANA UŽIVATELE

Z pohledu uživatele existují čtyři disciplíny počítačové bezpečnosti.

Jedná se o **správu identity**, čímž je míněno využívání čipových karet, účtů, hesel a práv s nimi spojených.