1. INFORMAČNÍ MANAGEMENT

Petr HRŮZA

1.1 Úvod

Zbožím dnešní doby se stávají stále častěji informace. Informace a podpůrné procesy, systémy a sítě jsou důležitými aktivy organizace. Vymezení, zavádění, podpora a zlepšování bezpečnosti informací může být zásadní pro udržení konkurenceschopnosti, peněžních toků, ziskovosti, právní shody a dobrého jména organizace.

Více než třetina firem na celém světě má informační systém zranitelný z hlediska bezpečnostních incidentů. Rozvíjející se organizace a jejich informační systémy jsou vystavovány bezpečnostním hrozbám z různých zdrojů, včetně počítačových podvodů, špionáže, sabotáže, vandalizmu, požárů a povodní. Zdroji škod jsou počítačové viry, útoky hackerů a útoky typu odepření služby. Ty jsou stále častější, roste jejich nebezpečnost a sofistikovanost.

Bezpečnost informačních systémů, která může být dosažena technickými prostředky, je nedostačující a měla by být doplněna odpovídajícím řízením a postupy. Bezpečnost informací lze dosáhnout implementací soustavy opatření, která mohou existovat ve formě pravidel, postupů, procedur, programových a hardwarových funkcí. Řízení bezpečnosti informací také vyžaduje spoluúčast všech zaměstnanců organizace. V neposlední řadě může být potřebná i rada od specialistů z jiných organizací.

1.2 Informační management

S pojmem informační management se lze setkat v různých souvislostech, doposud ale není jednoznačně ustálen jeho význam. Za **informační management lze chápat jako skupinu osob,** která je zodpovědná za informační systém organizace. Dalším významem tohoto pojmu, a na něj je zde kladen větší důraz, je proces výstavby a provozu informačních systémů organizace. Tento pohled se blíží pojetí informačního managementu v komerční sféře. V bezpečnostním prostředí se objevují další výklady pojmu informační management, např. předpis[1] uvádí, že: „*Informační management je soubor popsaných způsobů získávání informací a jejich využívání včetně databází důležitých informací a prostředí tvořeného KIS*“, ale také ve slovníku pojmů[2]: „*informační management - je to nepřetržité poskytování důležitých informací správné osobě ve správný čas v použitelné podobě za účelem zlepšení znalosti situace a rozhodovacího procesu*“. Obsah posledních dvou definicí informačního managementu spíše zdůrazňuje zajištění informační podpory, než procesy správného budování a provozu informačních systémů.

Informační management v procesním pojetí zahrnuje procesy výstavby, správy a řízení informačního systému organizace. Informačním systémem se však nechápe pouze počítačově orientovaný informační systém, realizující hlavní činnosti organizace, ale i

[1] Pub-53-01-1 Velení a řízení v operacích. Vyškov : SD ŘVD 2006, 76 str.
[2] Pub-53-01-1 Velení a řízení v operacích. Vyškov : SD ŘVD 2006, 191 str.

další subsystémy zajišťující v organizaci informační podporu řízení. Dalším příkladem je systém zveřejňování důležitých informací zaměstnancům organizace, zpravidla realizovaný prostřednictvím úřední desky. Informační management má v tomto pojetí za úkol systemizovat a zajišťovat všechny důležité informační činnosti a procesy, které zabezpečují řízení a chod v organizaci. Nezahrnuje pouze činnost počítačově orientovaných informačních systémů, ale i činnosti realizované tradičním způsobem. Obsah informačního managementu netvoří pouze procesy výstavby a provozu počítačově orientovaných informačních systémů, ale i vydávání různých metodik, směrnic, předpisů a dalších interních normativních aktů, obsahujících pravidla a způsoby práce s informacemi. Součástí informačního managementu je i specifikace informační kultury, tedy pravidel práce s informacemi, aby např. nedocházelo k informačnímu přetěžování zaměstnanců plošným rozesíláním e-mailů, nebo se v kancelářích například nevršily papírové dokumenty. V současné době se ve většině organizací završuje etapa informatizace, proto je hlavní pozornost informačního managementu zaměřena na procesy zavádění a provozu informačních systémů. V dalším období se očekává větší důraz na operační aspekty informačních systémů, na jejich lepší využití pro podporu řízení a zejména na restrukturalizaci bezpečnostních činností založených na využití potenciálu informačních a komunikačních technologií.

Informační management je manažerský obor, který systémově rozvíjí poznatky o účelném využití informačních procesů, technologií a specialistů k informační podpoře chodu organizace. Současný informační management využívá nejnovějších informačních a komunikačních technologií, projektuje a implementuje informační systémy na podporu manažerských funkcí a rolí, poskytuje informační služby subjektům organizace a zejména vedoucím pracovníkům – manažerům na všech úrovních řízení. Informační management je zaměřen na aplikaci informačních a komunikačních technologií v informačních systémech a v komunikačních a informačních službách. Současný informační management má ve firmě (organizaci) delegovány kompetence k zjišťování potřeb a volbě efektivního způsobu informatizace, na kterých se podílí.

Informační management je také chápán jako **nepřetržité poskytování důležitých informací** správné osobě ve správný čas v použitelné podobě za účelem zlepšení znalosti situace a rozhodovacího procesu. Informační management zahrnuje procesy správy a řízení informačního systému organizace. Je souhrnem koncepčních, plánovacích, řídících a kontrolních činností, zaměřených na výstavbu a provoz informačního systému organizace. Informačním systémem se v širším pojetí rozumí jak počítačově orientovaný informační systém, tak systém využívající tradiční informačních a komunikačních technologií. Důležitým aspektem informačního managementu je využití možností informačních a komunikačních technologií k zajištění informační podpory řízení. Součástí informačního managementu je zpracování dokumentů, nezbytných pro realizaci výstavby a provozu informačního systému organizace.

1.3 Obsah informačního managementu

Informační management respektuje a využívá nejnovější poznatky managementu jako takového a tvůrčím způsobem je uplatňuje v oblasti informačního systému organizace. Informační management zahrnuje procesy správy a řízení informačního systému organizace. Je souhrnem koncepčních, plánovacích, řídících a kontrolních činností, zaměřených na výstavbu a provoz informačního systému organizace. Důležitým aspektem informačního managementu je využití možností informačních a

komunikačních technologií k zajištění informační podpory řízení. Součástí informačního managementu je zpracování dokumentů, nezbytných pro realizaci výstavby a provozu informačního systému organizace.

Má-li být v organizaci informační systém vyvážený a odpovídající jejím potřebám, měly by v organizaci probíhat **procesy informačního managementu**. Za realizaci informačního managementu by měl zodpovídat informační manažer, podporovaný činností svého týmu pracovníků. Informační manažer je schopen vnímat potřeby organizace komplexně, dokáže provést popis a formulaci procesů, zorganizovat jejich návaznost a optimalizovat informační podporu. Vlivem jeho úsilí dochází k zlepšení činnosti informačního systému, zkvalitnění informační podpory a v konečném důsledku i zefektivnění činnosti organizace. Je třeba zdůraznit, že pro organizaci není informační systém cílem ale nástrojem k dosažení jejích cílů. Informační manažer by měl mít na paměti, že informační systém se výrazným způsobem dotýká struktury a způsobu řízení organizace.

Důležitou součástí informačního managementu je oblast zkoumání informačních potřeb uživatelů. Specifikace cíle, uvědomění si toho, co v organizaci potřebujeme z hlediska informací, to vše nám umožňuje lépe rozpracovat předmětnou oblast, navrhnout a upřesnit funkčnost informačního systému i zajistit jeho realizaci. Obdobný názor zastává i Tvrdíková[3], když uvádí: *„Vysoké investice do moderních informačních systémů a informačních technologií nejsou automatickou zárukou jejich efektivnosti. Zavádění informačních systémů a informačních technologií bez jasného cíle a bez cílevědomého vytváření podmínek pro jejich rozvoj a efektivní užívání nemá smysl“.* Výsledkem tvůrčích činností v oblasti informatiky může být i inovativní řešení, umožňující dosáhnout výsledné informační podpory nebo i činnosti organizace s podstatně nižšími náklady a lidskými zdroji.

1.4 Zásady, metody a nástroje informačního managementu

Zásady informačního managementu

Při realizaci procesů informačního managementu je vhodné respektovat určité zásady, které vychází ze složitosti výstavby informačních systémů a současně potřeb informační podpory velení a řízení. Zásadou se přitom rozumí určitý princip, nebo myšlenka či nepochybné východisko, ověřené praxí, jehož uplatnění umožní dosáhnout efektivního a optimálního výsledku. Uplatnění zásad probíhá v celém životním cyklu informačních systémů. Mezi základní zásady informačního managementu patří komplexnost, efektivnost, trvalost a přiměřenost.

- Zásada ***komplexnosti*** **-** umožňuje vidět organizaci v komplexu, jako jednotu cílové funkce organizace, procesů a informačních potřeb pracovníků a informačního systému jako nástroje realizace informační podpory.

- Zásada ***efektivnosti*** **-** zajišťuje, že náklady na informační systém odpovídají výsledné informační podpoře.

---

[3] Tvrdíková, M. *Zavádění a inovace informačních systémů ve firmách*. 1. vydání. Praha: Grada, 2000, 92 str.

- Zásada ***trvalosti*** **-** evokuje v informačním managementu trvalý zájem o zlepšení činnosti informačního systému.

- Zásada ***přiměřenosti*** **-** umožňuje zajistit, aby byla v organizaci přiměřená informační podpora.

Metody informačního managementu

V rámci životního cyklu informačních systémů jsou řídícími a výkonnými pracovníky informačního managementu používány k dosažení cílů určité metody práce, které umožňují efektivní výkon činnosti. Mezi základní metody informačního managementu lze zařadit analýzu, syntézu, metodu systémového přístupu, metodu projektového řízení, optimalizace, auditu a operativního řízení. Dále uvedené metody patří mezi hlavní metody informačního managementu, netvoří však jejich úplný výčet.

- Metoda ***analýzy*** **-** představuje v obecném slova smyslu myšlenkový postup, rozkládající vymezený celek na jeho části.

- Metoda s***yntézy*** **-** představuje metodu spočívající v skládání, spojování, slučování částí do organického celku. Představuje opak analýzy.

- Metoda ***systémového přístupu*** **-** podporuje řešení problému systémovým pohledem, umožňujícím vidět výsledný systém jako jednotu prvků a vazeb mezi nimi.

- Metoda ***projektového přístupu*** **-** umožňuje přistupovat k přípravě a návrhu informačního systému jako k projektu, se všemi nezbytnými zásadami a přístupy.

- Metoda ***optimalizace*** **-** představuje proces hledání nejvhodnější konfigurace či nejvhodnějšího postupu vzhledem k zadaným kritériím.

- ***Audit*** **-** je metoda umožňující prověření či zhodnocení stavu a jeho srovnání se stavem požadovaným.

- Metoda ***optimálního řízení*** - je založena na trvalém monitorování stavu informačního systému a odstranění nedostatků jeho činnosti.

Nástroje informačního managementu

- ***Systém řízení informačního systému*** **–** je základním nástrojem informačního managementu. Určuje systém, kompetence, odpovědnosti, činnost orgánů informačního managementu v zajištění výstavby a provozu informačního systému.

- ***Systém řízení bezpečnosti informací*** **–** jedná se o část celého systému řízení, která je založená na přístupu k bezpečnostním rizikům, k ustavení, implementování, provozování, monitorování, přezkoumávání, spravování a

zlepšování bezpečnosti informací[4]. Zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, praktiky, postupy, procesy a zdroje[5].

- ***Informační strategie*** **–** Informační strategie představuje koncepční dokument, vyjadřující vizi, plán a rámec budování, provozu a využití informačního systému dané organizace.

- ***Předpis*** **-** reprezentuje interní normativní akt organizace, jehož cílem je specifikace pravidel a způsobů realizace typických, organizací plněných úkolů. Předpis obsahuje obecný návod na řešení problému. Jeho platnost nebývá časově omezena.

- ***Směrnice*** **-** představuje dokument, upřesňující na základě obecně platné legislativy a předpisů, jak realizovat určitou činnost v předmětné oblasti. měrnice je více konkrétní, zpracovává se za účelem regulace v dané organizaci. Platnost směrnice může být časově omezena na určité období.

- ***Provozní dokumenty*** **-** jsou dokumenty provozního, konfiguračního a uživatelského charakteru, obsahující konkrétní údaje nezbytné k zajištění informační podpory.

- ***Zpráva auditu*** **-** představuje nástroj obsahující informace o hodnocení konkrétní předmětné oblasti informačního systému. Na základě hodnocení jsou přijímána opatření k nápravě stavu. V delším časovém horizontu může sloužit řada hodnotících zpráv k hlubším analýzám a prognózám činnosti a vývoje informačního systému.

- ***Softwarové produkty*** - představují nástroje, umožňující informačnímu managementu podporu jejích činností. Pomáhají vést přehledy o použitých hardwarových a softwarových prostředcích informačního systému.

- ***Školení zaměstnanců*** - obsahuje konkrétní teoretické a praktické informace o určení, službách, architektuře a softwarových aplikacích informačního systému. Umožňuje uživateli získat konceptuální obraz možností a způsobů využití informačního systému k informační podpoře jeho činnosti.

- ***Nácvik*** **-** procvičení a sladění společného kolektivního využití informačního systému k zajištění cílové funkce organizace. Zpravidla se jedná o nácvik určité činnosti organizace.

1.5 Role a povinnosti informačního manažera

Informační manažeři (CIO - Chief Information Office) jsou právě ti vedoucí pracovníci, kteří jsou v organizaci hnací silou rozvoje informatizace. Jde o velmi odpovědnou manažerskou pozici, neboť informační manažer je zodpovědný za

[4] ČSN ISO/IEC 27000 - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník

[5] ČSN ISO/IEC 27001 - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

strategický rozvoj a bezpečnost informačních systémů. Informační manažer by měl být členem vrcholového vedení organizace. Proto bývá součástí top managementu firmy. Skupina informačních manažerů bývá často označována jako informační management organizace.

Informační manažer také obvykle řídí útvar informačních systémů ve firmě, jehož velikost pochopitelně záleží na velikosti firmy. V některých organizacích může roli informačního manažera zastávat představitel organizace nebo jeho náměstek s delegovanou pravomocí a odpovědností. Informační manažer musí mít přesně specifikovány své povinnosti a pravomoci na jednotlivých úrovních řízení.

Úkolem informačního manažera je odpovídat za řízení provozu i rozvoje informatiky v organizaci a slaďovat cíle organizace informačními a komunikačními technologiemi. Jeho odpovědností je plánování rozvoje informačních a komunikačních technologií, sledování trendů a provádění nákladových analýz informačních a komunikačních technologií, řízení bezpečnosti a rizik v oblasti informatiky a celkové vyvažování informačního managementu organizace.

Podobně jako u ostatních manažerů, je manažerským úkolem informačního manažera plánovat, vést, organizovat, rozhodovat a kontrolovat lidi, procesy a informace v oblasti informatiky. Informační manažer může delegovat část svých pravomocí a odpovědností na další vrcholové manažery či manažery nižších úrovní.

Pro informačního manažera platí, že stejně jako jakýkoliv jiný manažer musí splňovat odpovídající úroveň manažerských dovedností a může vystupovat ve více manažerských rolích. Pro popis rozsahu odpovědností a kompetencí informačního manažera se používá model CIO Wheel, který byl popsán v rámci zákona Clinger-Cohen Act v roce 1996, a který popisuje kompetence informačního manažera v deseti oblastech:

- Policy - politika, pravidla,
- Strategic planning - strategické plánování,
- Performance & Result based - výkonnost a orientace na výsledky,
- Process Improvement - zlepšování procesů,
- Capital Planning & Investment - investiční plánování,
- Leadership management - vedení lidí,
- Technology Assessment - hodnocení technologií (ICT),
- Security – bezpečnost,
- Architectures – architektura,
- Acquisition - nákup a získávání zdrojů.

Velice důležitou věcí informačního manažera, na kterou se v dnešní době snižování výdajů zapomíná, je možnost informačního manažera disponovat patřičným finančním

fondem na údržbu a rozvoj informačního systému a informačních a komunikačních technologií.

Informační manažeři musejí být obeznámeni s nejrůznějšími druhy rizik. S riziky uvnitř vlastního IT úseku, s riziky, která ohrožují organizaci jako celek, s riziky spojenými s používáním technologií a s riziky strategickými. Ze jmenovaných kategorií patří k nejvíce zanedbávaným rizikům poslední (rizika strategická). Informačnímu manažerovi často brání v naplňování jejich poslání nedostatečná souhra mezi úsekem IT a organizací jako celkem[6]. Informační manažer se navíc musí v dnešní době vyrovnávat se současnými trendy outsourcingu, které na jedné straně rozšiřují okruh povinností, ale zároveň na straně druhé omezují možnosti spojené s výkonem kontroly a dohledu. Jejich pozice se od dřívější doby zásadně změnila také s rozšířením využívání počítačů jednotlivými koncovými uživateli, které je spojeno se zvýšenými riziky.

Hlavní role informačního manažera:

- vytvářet vizi IS/IT a prosazovat ji,
- poznávat podnik a zejména jeho trhy a zákazníky,
- získávat důvěru v útvar pro IS/IT,
- pečovat o informační gramotnost pracovníků,
- dbát na systémovou vyspělost IS/IT v podniku,
- rozvíjet informační infrastrukturu.

Jaké že má povinnosti informační manažer? Informační manažer musí mít přesně specifikovány své povinnosti a pravomoci na jednotlivých úrovních řízení, neboť i řízení informačního systému se uskutečňuje, stejně jako řízení ostatních aktivit ve třech rovinách - operativní, taktické a strategické. Činnost informačního manažera se týká všech tří úrovní, přičemž v rovině operativního a taktického řízení jeho činnost spíše monitorovací a kontrolní, zatímco na úrovni strategického řízení jsou kladeny vysoké požadavky na jeho kvalifikaci, aktivitu a tvůrčí schopnosti[7].

Hlavní povinnosti informačního manažera na úrovni strategického řízení:

- příprava informační strategie,
- výběr dodavatelů a nákup informačních systémů a technologií,
- řízení financí informačních systémů a technologií.

Hlavní povinnosti informačního manažera na úrovni taktického řízení:

- dodržování legislativy,

---

[6] VÁGNEROVÁ, Daniela [et al.]. *Příručka manažera XII - Supertipy CIO = CIO super tips : manager's handbook.* Praha: TATE International, 2009. 302 s. ISBN: 978-80-86813-18-9

[7] Tvrdíková, M. *Zavádění a inovace informačních systémů ve firmách*. 1. vydání. Praha: Grada, 2000

- ochrana dat.

Hlavní povinnosti informačního manažera na úrovni operativního řízení:

- zajištění provozu,
- zajištění školení a podpory zaměstnancům,
- zajištění bezpečnosti provozu.

Informační manažer by měl mít komplexní manažerskou kvalifikaci se zvýšenou pozorností věnovanou počítačovým disciplínám. Je potřebné zdůraznit, že funkční náplň informačního manažera by neměla být specifikována pouze s technickou orientací. Jeho úkolem je sledovat a ověřovat kvalitu informačního a komunikačního systému a jím nabízených služeb z pohledu potřeb řídicích pracovníků i ostatních zaměstnanců tak, aby zaměstnanci firmy zvládali práci s informačním systémem a byli stále motivováni k jeho efektivnímu užívání.

Informační manažer by měl být členem vrcholového vedení firmy, protože má-li v souladu s globální strategií firmy zabezpečovat rozvoj informačního systému a informačních technologií po stránce organizační a finanční, potřebuje k tomu mít patřičné rozhodovací pravomoci.

1.6 Základní dokumenty informačního managementu

Základním koncepčním dokumentem informačního managementu je **Informační strategie**. Informační strategie je vizí informačního systému organizace. Je promyšleným cílem, jehož by chtěla firma v oblasti výstavby a provozu informačního systému dosáhnout. Podle Sodomka[8] *„Informační strategie ztělesňuje dlouhodobou orientaci podniku v oblasti informačních zdrojů, služeb a technologií. Jejím smyslem je podpořit realizaci cílů organizace a podnikových procesů pomocí IS/CT".* Příprava a rozvoj Informační strategie jsou důležité jak z pohledu účinného fungování informačního systému, tak z pohledu správného, systematického a cíleného vkládání investic do informačních a komunikačních technologií a programových prostředků. Další výhodou vypracování Informační strategie je i získání poměrně jasné představy o nárocích na možného dodavatele IS/ICT (informačního systému a informačních a komunikačních technologií).

Základem zpracování informační strategie je zhodnocení současného stavu informačního systému organizace, finančních a jiných možností organizace, obecného stavu informačních a komunikačních technologií. Bez správné informační strategie není možné plánovat využití informačních a komunikačních technologií ve firmě. Bohužel se v některých případech stává, že informační strategii tvoří pouze myšlenkový zámysl odpovědných řídících pracovníků bez hlubších a podrobnějších analýz a znalosti budoucí strategie firmy. I takový stav je možný, odpovídá mu ale i výsledný informační systém organizace. Tvrdíková[9] zastává názor, že: *„Ty firmy a*

---

[8] Sodomka, P. *Informační systémy v podnikové praxi*. 1. vydání. Brno: Computer Press, 2006. 352 s. ISBN: 80-251-1200-4

[9] Tvrdíková, M. *Zavádění a inovace informačních systémů ve firmách*. 1. vydání. Praha: GRADA, 2000, 41 s.

instituce, které budují svůj informační systém bez informační strategie, nemají jasný cíl svého snažení, a proto mají malou naději na jeho efektivní vybudování".

Dalšími dokumenty, navazujícími na informační strategii jsou dokumenty spojené s plánováním, organizováním a řízením výstavby a provozu informačních systémů. Na základě dobře zpracované informační strategie mají řídící orgány dostatek podkladů k přípravě potřebných plánů, projektů výstavby i provozních dokumentů.

Důležitou, ale doposud opomíjenou oblastí informačního managementu je oblast kontroly funkčnosti informačního systému. Žádný legislativní podklad její pravidelné provádění neukládá, tudíž je realizována sporadicky. Důvodem je i obtížná kvantifikovatelnost hodnocení kvality informační podpory a nedostatek potřebných metrik atd. Tak jak se metody auditu postupně prosadily jako nástroje kontroly v oblasti hospodaření, tak i v oblasti informačního managementu by jich mělo být stále více používáno. **Informační audit a audit informačního systému** jsou kontrolními nástroji, které informačnímu managementu napomáhají v oblasti kontroly předmětné oblasti. Umožňují zhodnocení naplnění informačních potřeb uživatelů i stavu informačního systému jako takového. Výsledky auditu, obsahující podrobné zhodnocení stavu, umožní managementu organizace pochopit podstatu příčin nedostatků a lépe navrhnout opatření k jejich eliminaci.

1.7 Informační strategie

Pojmem **Informační strategie** se obvykle označuje koncepční dokument, jehož obsahem je soubor doporučení, která v rámci organizace definují informační potřeby a způsob jejich zabezpečení v souladu s celkovou podnikatelskou strategií firmy tak, aby její realizací byly v organizaci vytvořeny podmínky pro úspěšné podnikání v konkurenčním prostředí. Informačními potřebami jsou pak míněny všechny aspekty související s automatizací procesů, zpracováním, vyhodnocováním, oběhem a výměnou dat a dokumentů, a to za účelem podpory podnikání, rozhodování a řízení společnosti. Cílem Informační strategie je tedy záměr optimalizovat podporu globálních cílů organizace, a to za pomoci moderních prostředků informačních a komunikačních technologií.

Úkolem **Informační strategie je stanovit vizi, cíle a hodnoty budoucího informačního systému a informačních technologií organizace**, nelézt cestu k realizaci a pomoci řídit přechod od současného k cílovému stavu informačních a komunikačních technologií. Informační strategie úzce souvisí s cíli firmy, které sleduje. Jako cíle můžeme chápat budoucí žádoucí stavy, kterých má být dosaženo.

Informační strategie představuje koncepční dokument, vyjadřující vizi, plán a rámec budování, provozu a využití informačního systému dané organizace. Informační strategie vychází a navazuje na globální strategii organizace. V globální strategii, jako nadřazeném dokumentu, se promyšleným způsobem, s perspektivou, vyjadřuje cílová funkce organizace, účel, výstup, produkce. Podnikatelské subjekty pak výrobní program, poskytované služby apod. Dále tvoří její obsah priority rozvoje, organizační struktura, plán modernizace, financování, personalistika atd. Globální strategie vymezuje celkový koncept úspěšného fungování organizace.

Informační strategie je hlavním nástrojem strategického řízení IS/IT. Je jednou z dílčích strategií, které navazují na globální strategii organizace a představuje dlouhodobou

orientaci organizace v oblasti informačních zdrojů, služeb a technologií. Jejím cílem je optimální podpora cílů organizace a organizačních procesů pomocí informačních technologií, v souladu s požadavky uživatelů a rychle se rozvíjejícími informačními technologiemi.

Cílem dokumentu[10] je stanovení globální strategie v oblasti informačních a komunikačních technologií, které se mají stát výkonným nástrojem pro podporu dosahování strategických cílů organizace. Informační strategie je rovněž základním nástrojem systémové integrace.

Důležitou součástí dokumentu je SWOT[11] analýza, jejíž výsledky jsou využity při určení kritických oblastí.

Dokument **Informační strategie** má obvykle následující **strukturu**:

- Úvod.
- Zdroje a východiska.
- Legislativní rámec a požadavky na IS.
- Výchozí stav – analýza stavu IS.
    1. Analýza veškerých vnitřních i vnějších podnikových procesů.
    2. Analýza pokrytí všech procesů automatizovaným zpracováním pomocí IS.
    3. Analýza technologického zabezpečení IS.
    4. Analýza informačních potřeb.
- Cílový stav.
- Transformace do cílového stavu (navrhnout postup, jak dosáhnout cílového stavu ze současných podmínek).
- Závěr.

Podle Kocha[12] Informační strategie obsahuje následující hlavní oblasti:

- určení vazeb mezi celkovou strategií firmy a informační strategií,

---

[10] http://www.advice.cz/produkty-a-sluzby/studie-a-analyzy/informacni-strategie/

[11] SWOT analýza je univerzální analytická technika zaměřená na zhodnocení vnitřních a vnějších faktorů ovlivňujících úspěšnost organizace nebo jiného hodnoceného systému. Přirozeně a nejčastěji je SWOT analýza používána při strategickém řízení organizace při hodnocení nějakého strategického záměru. Autorem SWOT analýzy je Albert HUMPHREY, který ji navrhl v šedesátých letech 20. století. V rámci SWOT analýzy se hodnotí vnitřní a vnější faktory. Vnitřní faktory zahrnují silné stránky (Strengths) a slabé stránky (Weaknesses) organizace/systému. Vnější faktory zahrnují příležitosti (Opportunities) a hrozby (Threats), které souvisí s okolním prostředím organizace/systému. SWOT je akronym z počátečních písmen anglických názvů jednotlivých faktorů. Podstatou SWOT analýzy je tedy identifikovat klíčové silné a slabé stránky organizace a klíčové příležitosti a hrozby vnějšího prostředí.

[12] KOCH, Miloš [et al.]. *Management informačních systémů*. Brno: Akademické nakladatelství CERM, 2010. 171 s. ISBN: 978-80-214-4157-6

- analýza dosavadního vývoje informačních technologií ve firmě,
- analýza a prognóza obecného vývoje informačních technologií,
- určení informačních zdrojů pro informační podporu systému řízení firmy,
- plán rozvoje informačního systému ve střednědobém a dlouhodobém horizontu,
- objem finančních a nefinančních zdrojů pro zajištění realizace strategie,
- přehled standardů, které budou při realizaci uplatňovány,
- návrh organizačních změn a metrik dosažení cílů,
- návrh kvalifikačních a rekvalifikačních programů,
- zásady pro vyhodnocování účinnosti realizace strategie,
- outsourcing strategie pro informační služby.

Vypracování Informační strategie je obvykle završeno oponentním řízením, kde se k předkládanému dokumentu vyjadřuje vedení organizace. Po případném zapracování připomínek a doplňků je dokument vedením schvalován. Pro následnou implementaci Informační strategie je podstatné, aby se s ní vedení společností ztotožnilo a dokázalo pro ni získat ostatní spolupracovníky a tak ji prosadilo v celé organizaci.

Pokud vytvořením Informační strategie je pověřena externí organizace, musí vždy dojít k velmi těsné součinnosti mezi ní a zadávající společností. Externí organizace nemůže být totiž nikdy schopná sama o sobě (bez součinnosti) Informační strategii vytvořit. Naopak se dá konstatovat, že Informační strategii si vytváří vždy uživatel budoucího informačního systému a že externí organizace je mu při její tvorbě pouze nápomocná. Pak je rolí externí organizace především při tvorbě strategie vést tvůrce po stránce metodické a odborné.

Pokud v organizaci je již zaveden jakýkoliv informační systém, **musí**[13] vlastnímu vytvoření Informační strategie předcházet audit IS/ICT. V každém případě pak Informační strategii předchází audit informačních potřeb. Na vlastní dokument by dále měla navázat **implementace Informační strategie**, tj. rozpracování Informační strategie do cílového uspořádání IS/ICT, stanovení plánu, jak cílového stavu dosáhnout a vlastní realizace plánu.

Účel Informační strategie pro firmy je možné shrnout v následujících bodech:

1. Je klíčovým podkladem ke směřování rozvoje firmy v oblasti IS/ICT.
2. Je důležitým podkladovým materiálem pro zpracování dokumentů, kterými firma oslovuje externí dodavatele IS/ICT.
3. Definuje vazby mezi všemi projekty ve firmě, včetně projektů pro rozvoj informačních technologií.

[13] http://www.cz-ckc.cz/informacni-strategie.html

4. Urychluje řešení zavádění IS/ICT.

5. Obsahuje koncepční podklady pro plánování nezbytných investic v oblasti IS/ICT na její pravidelnou údržbu.

Pro důsledné zajišťování informační strategie je potřebné určit jejího **zodpovědného reprezentanta** ve firmě. Roli reprezentanta zodpovědného za informační strategii firmy zastává obvykle **informační manažer**. Monitoruje situaci uvnitř i vně firmy a na základě důkladné analýzy svých poznatků dokáže posoudit riziko jednotlivých akcí celé informační strategie firmy.

Informační manažer nebo jiný subjekt, odpovědný za informační strategii (například externí firma) pak odpovídá za kvalitu specifikace klíčových informací pro podporu rozhodování řídících pracovníků firmy a výběr standardů, které chce firma uplatňovat při budování informačního systému. Na firmu musí pohlížet jako na celek, který se skládá z částí v neustálé vzájemné interakci. Důsledným systémovým přístupem tak zabezpečuje návaznost informační strategie na celkovou strategii firmy a její komplexnost.

Vypracování Informační strategie může mnohé firmy zbavit řady problémů, snižuje rizika ze zavádění a inovací IS/ICT a ve svém důsledku zvyšuje účinnost nových informačních systémů. Osobou zodpovědnou za informační strategie firmy je většinou informační manažer firmy.

1.8 Bezpečnostní a informační politika

Politika představuje stav a způsob fungování určitého systému. Politika se uskutečňuje cestou formulace zásad, pravidel, opatření atd. Bezpečnostní politika organizace např. vymezuje cíle bezpečnosti a způsob jakým mají být zajištěny, dále pravidla, normativy atd. Na jejím základě jsou zpracovány režimové směrnice organizace, zajištěna fyzická ostraha a budován elektronický bezpečnostní systém. Informační i bezpečnostní politiku je třeba chápat jako nekončící a stále se vyvíjející proces, který ovlivňují technologické, ekonomické, sociální, kulturní a organizační faktory.

První **informační politiky** vznikaly jako přímá odpověď na objevení specifických informačních technologií: tisk, telefon, rádio, počítač. Tyto politiky byly směřovány k jednotlivým technologiím a vedly k fragmentaci na jednotlivé věci. Ani dneska nevíme, zda je lepší mluvit o několika politikách nebo se pokusit je sjednotit v jeden trochu nesourodý celek.

Bezpečnostní politika je souhrn požadavků, potřeb, pravidel, směrnic, předpisů a zásad, které jsou definovány pro zabezpečení všech prvků informačního systému na všech úrovních přístupu odpovídajících potřebám a možnostem firmy. Bezpečnostní politika informačního systému musí definovat hlavní cíle při ochraně informací, stanovit způsob řešení bezpečnosti a určit pravomoc zodpovědnosti. Definuje východiska pro všechny další aktivity firmy v oblasti informační bezpečnosti[14]. Musí pokrývat všechny významné oblasti informační bezpečnosti. Při vytváření bezpečnostní politiky je potřeba

[14] JAŠEK, Roman. *Informační a datová bezpečnost*. 1. vydání. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. 140 s. ISBN: 80-7318-456-7

stanovit úroveň detailu, faktografický rozsah a rozsah dokumentu, úroveň podrobnosti, definovat základní principy, odpovědnosti a pravomoci. Vytvořením bezpečnostní politiky práce nekončí. Tuto politiku je potřeba přijmout a vyhlásit. Po schválení vrcholovým managementem je důležité, aby byli všichni zaměstnanci s dokumentem seznámeni.

Informační politika je dlouhodobá koncepce rozvoje informačních a komunikačních technologií. Informační politika je nikdy nekončící a stále se vyvíjející proces, který ovlivňují technologické, ekonomické, sociální, kulturní a organizační faktory. Základním kriteriem dělení jednotlivých informačních politik je způsob budování a provozování informačního systému organizace jako celku, případně autonomnost dílčích subsystémů (informačních systémů jednotlivých prvků organizace) a schopnost jejich vzájemné spolupráce. V konečném důsledku se jedná o způsob budování informačního systému organizace, organizační strukturu zajišťující toto budování, způsob financování výstavby a provozu informačních systémů a schopnost spolupráce jednotlivých informačních systémů. Možnost či nemožnost sdílení dat je jedním znaků informační politiky uplatněné v dané organizaci. Míra definování a uplatnění informační politiky je odrazem kvality informačního managementu v organizaci. Je-li informační politika trvale pěstována a prosazována, zlepšuje se vlastní informační podpora řízení a postupně vzniká informačně založená organizace.

1.9 Monitoring a audit informačního systému

Monitoring a audit informační bezpečnosti je nedílnou součástí procesu řízení informační bezpečnosti. Nedostatečná úroveň a absence monitoringu bývá příčinou, že bezpečnostní incidenty zůstávají dlouhou dobu neodhaleny a vzniklé škody pak mohou několikanásobně převýšit případné škody těchto incidentů odhalených včas. Monitoring stejně jako celý proces řešení bezpečnosti musí začít u analýzy největších rizik a sledování bezpečnostních událostí. Dodržování bezpečnostních standardů musí být tedy soustředěno do oblastí s největším rizikem.

Monitoring informačního systému

Společnost FreeDivision má na svých internetových stránkách velice výstižný citát: „*I nejspolehlivější bezpečnostní systém je pouze teoretickou obranou proti útokům, dokud není vyzkoušen v praxi. Samozřejmě nemá smysl čekat na skutečný útok, ideální je řízená zkouška robustnosti a spolehlivosti bezpečnostních opatření, kterými firma chrání citlivá data*“[15].

K provádění účinného **monitoringu** informačního systému je nejprve nezbytné vydefinovat celkový rozsah monitoringu. Je potřeba určit jaké informace, zdroje a citlivá místa mají být monitorována. Dále je důležité vydefinovat a rozdělit odpovědnosti za monitoring. Kdo co bude dělat a za co bude odpovídat vedení firmy, bezpečnostní manažer, vlastní a externí zaměstnanci.

Mezi způsoby monitoringu informačního systému patří penetrační testování, které je založeno na aktivním zjišťování a odhalování bezpečnostních slabin systému.

[15] FreeDivision s.r.o. , www.freedivision.com

Penetrační test je součást bezpečnostní analýzy ověřující úroveň bezpečnosti IT. Díky testu je možné odhalit chyby v zabezpečení informačních systémů či aplikací a je možné zabránit úniku informací, poškození či zneužití. Penetrační test je správným začátkem na cestě k optimálnímu zabezpečení sítě a k efektivnějším investicím do IT. Výstupem penetračních testů je podrobná zpráva, která popisuje nalezené zranitelnosti, rizika s odhadem jejich míry dopadu. Penetrační testy je dobré pravidelně opakovat.

Bezpečnostní a informační audit

I přes dobře nastavené provozní mechanizmy monitoringu informačního systému je potřeba, aby byl opakovaně prováděn nezávislý audit všech klíčových prvků a procesů informačních systémů a technologií. Audit umožňuje také získat přehled o výpočetní technice (hardware, software, sítě) instalované a využívané ve firmě. Tento ucelený přehled je také především vhodný při rozhodování o modernizaci počítačového vybavení a optimalizaci nákladů na rozvoj, provoz a správu výpočetní techniky.

Audit obecně chápeme jako kritickou analýzu nebo hloubkovou kontrolu se zaměřením na zlepšení procesů v organizaci. Audit může pomoci při stanovení a případně dosažení cílů organizace, pokud je prováděn jako systematicko-metodický přístup k systému řízení, kontroly a správy organizace. V dnešní době je audit chápán jako synonymum hloubkové kontroly pro specifické oblasti.

Audit informačního systému můžeme chápat jako **analýzu** informačního systému, jejímž cílem je posoudit, zda je systém ve shodě se stanovenými požadavky (uživatelskými, legislativními, kvalitativními, bezpečnostními, normalizačními apod.). Audit provádí nezávislá autorizovaná osoba nebo instituce, která nemá přímou odpovědnost za funkce prověřovaného systému. Audit můžeme vnímat také jako **záznam událostí a činností** vykonaných uživatelem nebo jeho jménem, důležitých z hlediska bezpečnosti informačního systému (tzv. bezpečnostní audit). Spolu s identifikací a autentizací slouží k určení zodpovědnosti při vyšetřování bezpečnostních incidentů.

Problematice norem auditu se kromě státních a národních standardizačních institutů věnuje Mezinárodní organizace pro standardizaci (ISO) a také profesně zaměřené instituce, např. Information Systems Audit and Control Association (ISACA). V České republice je to Společnost pro rozvoj informační gramotnosti (SPRIG).

Bezpečnostní audit je zhodnocení stavu bezpečnosti vůči vybranému standardu. Audit je prováděn fyzicky přímo na zkoumaném zařízení (např. serveru), nikoli vzdáleně po síti. Audit vyžaduje plný přístup ke zkoumaným zařízením a je prováděn za asistence administrátora. Hlavním cílem bezpečnostního auditu je zmapování aktuálního stavu bezpečnosti v rámci firmy, odhalení možných rizik a vytvoření základu pro případné ucelené bezpečnostní řešení (audit IS, penetrační testy, analýza rizik). Základem je pasivní sběr informací o konfiguraci a nastavení informačního systému. Posléze následuje vyhodnocení těchto informací a vyvození závěrů. Výsledkem bezpečnostního auditu je porovnání zjištěných hodnot vůči hodnotám doporučeným a samostatná zpráva o každém zařízení.

Cílem **informačního auditu** je zhodnocení stavu informační podpory organizace jako takové, abstrahující od hodnocení informačního systému. V jeho rámci se identifikují informace, které jsou nezbytné k řízení organizace, jsou-li poskytovány informačními zdroji, nedochází-li k duplicitě zdrojů v poskytování informací případně jejich absenci.

Podle[16] může informační audit zahrnovat následující kroky nebo fáze:

1) plánování,
2) sběr údajů,
3) analýzu údajů,
4) hodnocení údajů,
5) komunikační doporučení,
6) implementační doporučení.

Firma by měla provádět audit informačního systému v plánovaných intervalech tak, aby si vždy minimálně dokázala odpovědět na následující otázky:

- Vyhovuje stávající IS všem našim požadavkům?
- Je náš IS zaveden a udržován efektivně?
- Funguje nám IS tak, jak se od něho očekává?

Mimo již dva zmíněné audity existují ještě **technický audit, audit informační strategie a legislativní audit**. Výstup **technického auditu** (audit HW a SW vybavení, audit infrastruktury) slouží jako podklad pro odhad (ochranu) investic do infrastrukturních komunikačních systémů. Výstup může obsahovat návrh na rozšíření či úpravu konfigurace systému, případně změnu technologie. Výsledkem **auditu informační strategie** je podklad a stanovení kritérií pro správnou strategii v oblasti informačních technologií vzhledem k potřebám a podnikatelským záměrům firmy (koncepce, ohodnocení spokojenosti uživatelů a zákazníků, rozbor funkčnosti a popis informačního systému). **Legislativní audit** sumarizuje základní informace o informačním systému a ověřuje, zda informační systém je ve shodě s požadavky zákonů, které se týkají bezpečnosti dat a informačních systémů.

Audit dále dělíme na **interní a externí audit**[17]. Cílem **interního auditu** je ujistit se, že celková ochrana systému je přiměřená k rizikům, která na systém působí. Výsledkem interního auditu je podklad pro management k modifikaci a optimalizaci firemní strategie. Interní audit je většinou definován pro potřeby vedení společnosti a je závislý na dohodě s vedením. S výhodou lze u interního auditu využít výsledky monitoringu. **Externí audit** slouží k ověření podstatných vlastností systému nezávislým subjektem, provádí ho specialisté externí organizace na základě objednávky nebo jako součást správního řízení. Rozsah a výstup externího auditu může být stanoven legislativně.

Program auditů musí být naplánován s ohledem na stav a význam auditovaných procesů a oblastí a také s ohledem na výsledky předchozích auditů. Musí být definována kritéria auditů, jejich rozsah, četnost a metody. Výběr auditorů a vlastní provedení auditů musí

---

[16] Henczel. S. *The Information Audit: A Practical Guide*. 1. vydání. Munich : K. G. Saur 2001. ISBN 3598243677

[17] NĚMEC, Petr. *Audit informačních systémů nebo penetrační testy?* In sborník SYSTEMS INTEGRATION 2008, str. 87

zajistit objektivitu a nestrannost procesu auditu. Auditoři nesmí auditovat (prověřovat) svou vlastní práci. Odpovědnosti a požadavky na plánování a provedení auditů, na hlášení výsledků a udržování záznamů musí být definovány dokumentovaným postupem. Vedoucí zaměstnanci odpovědní za oblast, která je předmětem auditu, musí zajistit, že kroky na odstranění zjištěných nedostatků a jejich příčin budou prováděny bez zbytečného odkladu[18].

Bez monitoringu a auditu není celkové řízení bezpečnosti komplexní. Řada firem ale na tuto skutečnost často zapomíná a podceňuje ji.

1.10 Provozní řád informačního systému

Povinnost atestovat informační systém dle standardu pro životní cyklus informačních systémů si v dnešní době vynucuje pečlivější přístup k této problematice. Co by určitě měl takový provozní řád obsahovat? Kdo všechno se jím musí ve firmě řídit a kdo ne? Neměl by být každý uživatel vyškolen a neměl by prokázat způsobilost s užíváním IT a podepsat Provozní řád informačního systému dané firmy dříve, než mu bude přidělen přístup do informačního systému? Může zaměstnanec pracovat s informačním systémem, aniž by absolvoval aspoň základní školení a podepsal, že byl obeznámen s Provozním řádem informačního systému? To jsou základní a důležité otázky administrátory firmy. Obecně platí to, že čím větší firma, tím lepší ošetření práce s IS pomocí vnitřních směrnic.

Jaké části by mohl nebo spíše měl takový provozní řád obsahovat?

1. ÚVODNÍ USTANOVENÍ

    Definice základních pojmů

    Správce informačního systému

    Provozovatel informačního systému

    Nakládání s informacemi

    Struktura informačního systému

    Odpovědnost organizačních a řídících struktur

2. PROVOZNÍ ŘÁD

    Obecné zásady práce s výpočetní technikou

    Práva a povinnosti uživatele

    Bezpečnostní zásady

    Provozní doba sítí

---

[18] Norma ČSN ISO 19011, *Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu*, může být dobrým zdrojem doporučení, jak provádět audity IS.

Pohotovost pro uživatele

Semináře, školení

Archivace datových souborů

Elektronická pošta

Antivirová bezpečnost

Používání Internetu

Vytváření přístupů uživatelů k informačnímu systému

Změna a rušení přístupů uživatelů k informačnímu systému

Publikování informací

3. ZÁVĚREČNÁ USTANOVENÍ

Určuje většinou platnost Provozního řádu, jeho novelizaci atp.

4. PŘÍLOHY

Soupis případných příloh k Provoznímu řádu (Například: Výkladový slovník IS, Předávání dat IS, Protokol o instalaci klientského počítače, Protokol operativní evidence, Evidenční list, Požadavek na vytvoření přístupu k informačnímu systému pracovníka, Požadavek na zrušení přístupu a převod dat).

Dá velkou práci to dobře vymyslet a napsat, ale vyplatí se to.

1.11 Systém řízení bezpečnosti informací

V dnešní době se již žádná organizace nemůže obejít bez řízení bezpečnosti informací. Bezpečnost informací se stala nedílnou součástí každodenního řízení a vnitřní kultury každé organizace. Abychom byli schopni řízení bezpečnosti informací cíleně, účinně a účelně rozvíjet, je třeba tento prvek řízení vnímat jako systém řízení bezpečnosti informací. Bezpečnost informačního systému je souhrn opatření k zabezpečení provozu informačního systému podle stanovených zásad a pravidel k ochraně jejich dat před neoprávněným narušením, změnou, zneužitím a užíváním.

Systém řízení bezpečnosti informací (ISMS - Information Security Management System) poskytuje model pro ustavení, implementování, zpracovávání, monitorování, přezkoumávání, udržování a zlepšování ochrany informačních aktiv, aby byly dosaženy cíle organizace na základě posouzení rizik a úrovních akceptace rizik organizace navržených k efektivnímu ošetření a řízení rizik[19]. Jednoduše lze říci, že ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození. Úkolem ISMS je zavést pravidla a postupy pro řízení

[19] ČSN ISO/IEC 27000 - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník

informační bezpečnosti organizace. Pro ISMS v rámci organizace musí být jednoznačně popsána organizace řízení, odpovědnost za informační bezpečnost řídících pracovníků všech stupňů, odborných orgánů a rolí v systému bezpečnosti informací. Interpretace a implementace jednotlivých doporučení se však může výrazně lišit podle rozsahu systému, počtu uživatelů, způsobu zpracování dat, jejich hodnoty a především podle reálných bezpečnostních rizik. ISMS nebývá v malých a středních firmách popsána tak detailně, jako je tomu ve velkých firmách, zejména nadnárodních organizacích.

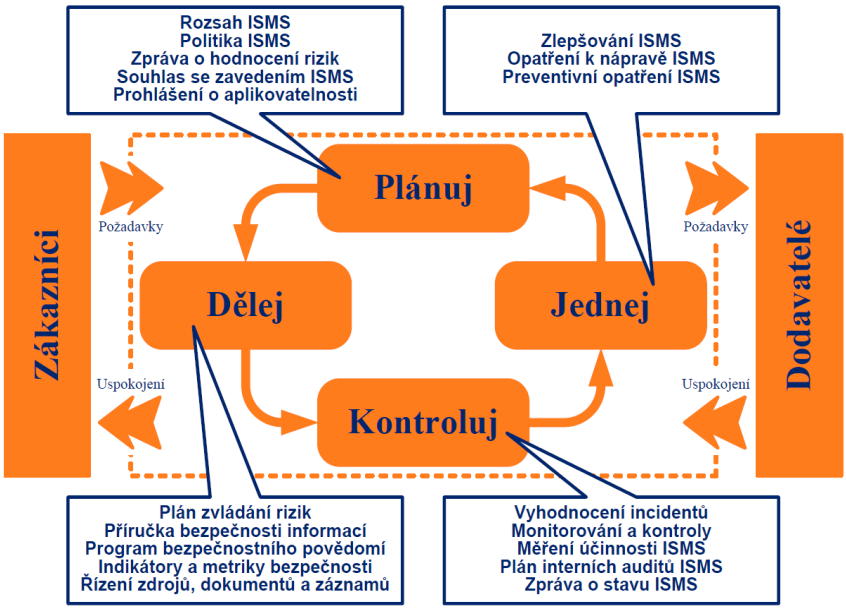
Stručně řečeno systém řízení bezpečnosti informací (ISMS) je:

- procesní přístup pro vybudování, zavedení, provozování, monitorování, udržování a zlepšování efektivnosti bezpečnosti v organizaci,

- soustava opatření ve formě pravidel, postupů, procedur, organizační struktury, programových a hardwarových funkcí.

Ideální by bylo, kdyby každá firma dokázala ustavit, zavést, provozovat, monitorovat, přezkoumávat, udržovat a soustavně zlepšovat dokumentovaný systém řízení bezpečnosti informací firmy, a to v kontextu všech činností a rizik.

Systém řízení bezpečnosti informací je podobně jako ostatní systémy řízení založen na modelu **PDCA (Plánuj – Dělej – Kontroluj – Jednej -** z anglického názvu Plan-Do-Check-Act neboli PDCA)**.** Model PDCA může být aplikován na všechny procesy ISMS. Model PDCA také znázorňuje všechny principy nezbytné pro řízení bezpečnosti informačních systémů a sítí.



Obr. 1: Model PDCA pro řízení bezpečnosti informací podle ČSN ISO/IEC 27001[20]

Plánuj (ustavení ISMS)- cílem je ustavení politiky ISMS, procesů a postupů souvisejících s managementem rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly

[20] Novák, L., Požár, J. *Systém řízení informační bezpečnosti*. In *Pracovní příručka bezpečnostního manažera*. 1. vydání. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2011, 104 str., ISBN: 978-80-7251-364-2

výsledky v souladu s celkovou politikou a cíli organizace. Stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření.

Dělej (zavádění a provoz ISMS) – cílem je zavedení a využívání politiky ISMS, opatření, procesů a postupů neboli účelně a systematicky prosadit vybraná bezpečnostní opatření do chodu organizace.

Kontroluj (monitorování a přezkoumání ISMS) – cílem je posouzení a pokud je to možné i měření výkonu procesu vůči politice ISMS a hlášení výsledků vedení organizace k přezkoumání. Zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nevyhovující stránek řízení bezpečnosti informací.

Jednej (udržování a zlepšování ISMS) – cílem je přijetí opatření k nápravě a prevenci opatření, založených na výsledcích interního auditu ISMS. Přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS ať už soustavným zlepšování systému nebo odstraňování zjištěných slabin a nedostatků.

Jednoduše řečeno, v první etapě (Plánuj) je potřeba systém vhodně naplánovat, ve druhé etapě (Dělej) je potřeba naplánované prosadit, ve třetí etapě (Kontroluj) je potřeba provádět pravidelné kontroly a vyhodnocovat je a nakonec ve čtvrté etapě (Jednej) je potřeba celý systém zlepšovat a zkvalitňovat.

1.12 Shrnutí

Informační management lze chápat jako skupinu osob, která je zodpovědná za informační systém organizace. Dalším významem tohoto pojmu je proces výstavby, správy, provozu a řízení informačního systému organizace. Za realizaci informačního managementu by měl zodpovídat informační manažer.

Při realizaci procesů informačního managementu je vhodné respektovat určité zásady, které vychází ze složitosti výstavby informačních systémů a současně potřeb informační podpory řízení. Uplatnění zásad probíhá v celém životním cyklu informačních systémů. Mezi základní **zásady informačního managementu** patří komplexnost, efektivnost, trvalost a přiměřenost.

V rámci životního cyklu informačních systémů jsou řídícími a výkonnými pracovníky informačního managementu používány k dosažení cílů určité metody práce, které umožňují efektivní výkon činnosti. Mezi základní **metody informačního managementu** lze zařadit analýzu, syntézu, metodu systémového přístupu, metodu projektového řízení, optimalizace, auditu a operativního řízení.

Informační manažeři jsou ti vedoucí pracovníci, kteří jsou v organizaci hnací silou rozvoje informatizace. Jde o velmi odpovědnou manažerskou pozici, neboť informační manažer je zodpovědný za strategický rozvoj a bezpečnost informačních systémů. Informační manažer by měl být členem vrcholového vedení organizace. Proto bývá součástí top managementu firmy. Skupina informačních manažerů bývá často označována jako informační management organizace.

Základním koncepčním dokumentem informačního managementu je **Informační strategie**. Informační strategie je vizí informačního systému organizace. Je promyšleným cílem, jehož by chtěla firma v oblasti výstavby a provozu informačního

systému dosáhnout. Základem zpracování informační strategie je zhodnocení současného stavu informačního systému organizace, finančních a jiných možností organizace, obecného stavu informačních a komunikačních technologií. Informační strategie vychází a navazuje na globální strategii organizace.

Bezpečnostní politika je souhrn požadavků, potřeb, pravidel, směrnic, předpisů a zásad, které jsou definovány pro zabezpečení všech prvků informačního systému na všech úrovních přístupu odpovídajících potřebám a možnostem firmy. Bezpečnostní politika informačního systému musí definovat hlavní cíle při ochraně informací, stanovit způsob řešení bezpečnosti a určit pravomoc zodpovědnosti. Definuje východiska pro všechny další aktivity firmy v oblasti informační bezpečnosti.

Důležitou, ale doposud opomíjenou oblastí informačního managementu je oblast kontroly funkčnosti informačního systému. **Monitoring a audit** informační bezpečnosti je nedílnou součástí procesu řízení informační bezpečnosti. Monitoring stejně jako celý proces řešení bezpečnosti musí začít u analýzy největších rizik a sledování bezpečnostních událostí. I přes dobře nastavené provozní mechanizmy monitoringu informačního systému je potřeba, aby byl opakovaně prováděn nezávislý audit všech klíčových prvků a procesů informačních systémů a technologií. Bez monitoringu a auditu není celkové řízení bezpečnosti komplexní.

V dnešní době se již žádná organizace nemůže obejít bez řízení bezpečnosti informací. Bezpečnost informací se stala nedílnou součástí každodenního řízení a vnitřní kultury každé organizace. Abychom byli schopni řízení bezpečnosti informací cíleně, účinně a účelně rozvíjet, je třeba tento prvek řízení vnímat jako systém řízení bezpečnosti informací. Bezpečnost informačního systému je souhrn opatření k zabezpečení provozu informačního systému podle stanovených zásad a pravidel k ochraně jejich dat před neoprávněným narušením, změnou, zneužitím a užíváním. **Systém řízení bezpečnosti informací** poskytuje model pro ustavení, implementování, zpracovávání, monitorování, přezkoumávání, udržování a zlepšování ochrany informačních aktiv, aby byly dosaženy cíle organizace na základě posouzení rizik a úrovních akceptace rizik organizace navržených k efektivnímu ošetření a řízení rizik.

Literatura:

1) Monografické publikace (knihy)

[1] DOUCEK, Petr; NEDOMOVÁ, Lea; NOVÁK, Luděk; SVATÁ, Vlasta. *Řízení bezpečnosti informací.* Druhé přepracované vydání, Praha: Professional Publishing, 2011, ISBN 978-80-7431-050-8.

[2] HENCZEL., Susan. The Information Audit: *A Practical Guide*. 1. vydání. Munich: K. G. Saur, 2001. ISBN: 3598243677.

[3] JAŠEK, Roman. *Informační a datová bezpečnost.* 1. vydání. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. 140 s. ISBN: 80-7318-456-7.

[4] KOCH, Miloš [et al.]. *Management informačních systémů*. Brno: Akademické nakladatelství CERM, 2010. 171 s. ISBN: 978-80-214-4157-6.

[5] LUKÁŠ, Luděk; HRŮZA, Petr; KNÝ, Milan. *Informační management v bezpečnostních složkách.* 1. vyd. Praha: AVIS, 2008. 214 s., ISBN 978-80-7278-460-8.

[6] MOLNÁR, Zdeněk. *Efektivnost informačních systémů*. 2. vydání. Praha: Grada, 2001, 69 s.

[7] SODOMKA, Petr. *Informační systémy v podnikové praxi*. 1. vydání. Brno: Computer Press, 2006. 352 s. ISBN: 80-251-1200-4.

[8] TVRDÍKOVÁ, Milena. *Zavádění a inovace informačních systémů ve firmách*. 1. vydání. Praha: Grada, 2000, 92 s.

[9] TVRDÍKOVÁ, Milena. Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů. 1. vyd. Praha : Grada, 2008. 173 s. ISBN: 978-80-247-2728-8.

[10] VÁGNEROVÁ, Daniela [et al.]. *Příručka manažera XII - Supertipy CIO = CIO super tips : manager's handbook*. Praha: TATE International, 2009. 302 s. ISBN: 978-80-86813-18-9.

2) Příspěvek ve sborníku

[11] HANÁČEK, Petr; STAUDEK, Jan. *Bezpečnost informačních systémů: Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000. 127 s.

[12] NOVÁK, Luděk; POŽÁR, Josef. *Systém řízení informační bezpečnosti*. In *Pracovní příručka bezpečnostního manažera*. 1. vydání. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2011, s. 104. ISBN: 978-80-7251-364-2.

3) Webová stránka

[13] www.freedivision.com, [online]. [cit. 2012-5-4]. Penetrační testy. Dostupné z WWW: <http://www.freedivision.com/files/penetracni_testy.pdf>.

[14] NĚMEC, Petr. *Audit informačních systémů nebo penetrační testy?* In sborník *SYSTEMS INTEGRATION 2008,* str. 86-92 [online]. [cit. 2012-5-5]. Dostupné z WWW: <http://si.vse.cz/archive/proceedings/2008/audit-informacnich-systemu-nebo-penetracni-testy.pdf>.

4) Norma

[15] ČSN ISO/IEC 27000 - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

[16] ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky.