Jaroslav Mlýnek
Informační bezpečnost

Pokroky matematiky, fyziky a astronomie, Vol. 51 (2006), No. 2, 89--98

Persistent URL: http://dml.cz/dmlcz/141305

Informační bezpečnost

Jaroslav Mlýnek, Liberec

1. Úvod

V současné době patří informace zpracované, přenášené a uložené v elektronické formě mezi nejcennější aktiva obchodních společností, výrobních firem, jsou nepostradatelné ve státní správě a ostatních organizacích. Z toho vyplývá přirozený požadavek jejich zabezpečení, tj. zajištění jejich důvěrnosti, dostupnosti a obsahové neporušenosti (integrity). Každá organizace je povinna chránit své informace v rámci platné legislativy a závazků vyplývajících ze smluv se spolupracujícími organizacemi a současně by měla své informace chránit i ve vlastním zájmu. V tomto článku se řeší problematika zabezpečení elektronických informací.

Zabezpečení informací se zpravidla provádí v rámci informačního systému (dále IS) dané organizace nebo její části. IS integruje informační základnu (data), technické a programové vybavení, interní předpisy a manuály, uživatele a správce.

V následujícím odstavci se zaměříme na kryptografické nástroje, které mají nezastupitelné místo při realizaci zabezpečení elektronických informací.

2. Kryptografické nástroje

Kryptografické nástroje umožňují především zajistit důvěrnost, integritu a autentičnost informací, nepopiratelnost původu informací (autor dokumentu nemůže později popřít své autorství) a autentizaci entit (uživatele IS, počítače, počítačové aplikace).

Kryptografie (tvorba bezpečnostních algoritmů) je součástí vědního oboru kryptologie, zahrnujícího také oblast kryptoanalýzy (analýza bezpečnostních algoritmů).

Počátky kryptografie sahají hluboko do historie a jsou spojeny se vznikem písma. Jednalo se především o šifry umožňující utajení zpráv a jejich užití bylo doménou vojenských a špionážních služeb i diplomatických kruhů. Šifrovací algoritmy byly založeny především na substituci a transpozici znaků.

Vývoj kryptografie v první polovině 20. století byl významně ovlivněn zavedením telegrafu jako běžného komunikačního prostředku. V té době byly vyvíjeny mechanické a elektromechanické šifrovací stroje. Například německá armáda užívala za 2. světové války známý šifrovací stroj Enigma a Anglie vyvinula velké úsilí k jeho úspěšné kryptoanalýze. Americká armáda používala v té době stroj Sigaba, který se nepodařilo Němcům rozluštit.

RNDr. Jaroslav Mlýnek, CSc. (1957), katedra matematiky a didaktiky matematiky, Fakulta pedagogická, Technická univerzita v Liberci, Hálkova 6, 461 17 Liberec 1, e-mail: jaroslav.mlynek@tul.cz

Kryptoanalýza šifrovacích strojů významně ovlivnila vznik a následný vývoj elektronických počítačů. V poválečném období si všechny světové mocnosti vybudovaly kryptografická a kryptoanalytická centra.

Nové možnosti rozvoje kryptografie přicházejí s rozvojem výpočetní techniky v 2. polovině minulého století. Moderní kryptografické metody jsou založeny nejčastěji na teorii čísel.

Mezi základní kryptografické nástroje patří zejména jednosměrné funkce, kontrolní kryptografické součty, šifrovací algoritmy a algoritmy digitálního podpisu.

2.1. Jednosměrné funkce

Nechť A i B jsou množiny posloupností bitů obsahujících 0 a 1. Prvky x množiny A reprezentují elektronické soubory. Pak funkci $f\colon A \to B$ nazveme jednosměrnou, jestliže pro každé $x \in A$ je snadný výpočet funkční hodnoty $f(x)$; avšak pro libovolnou hodnotu $y \in f(A)$ je obtížné nalézt vzor (není technicky proveditelné) $x \in A$ tak, aby platilo $y = f(x)$. Současně k danému $x_1 \in A$ není možné v reálném čase určit takové $x_2 \in A$, aby platilo $x_1 \neq x_2$ a $f(x_1) = f(x_2)$.

Za příklad jednosměrné funkce lze považovat funkci danou vztahem

$$f(x) = g^x \bmod n, \tag{2.1}$$

kde n je velké prvočíslo a g je primitivní kořen prvočísla n (viz [6]). Pak i pro velké celé číslo x lze snadno vypočítat hodnotu $f(x)$, avšak zpětné určení hodnoty x z $f(x)$ (tj. výpočet diskrétního logaritmu) není v reálném čase realizovatelné.

V kryptografii se také užívají jednosměrné funkce s „padacími vrátky“ (anglicky trap-door one-way function). Uvedený typ jednosměrné funkce lze invertovat pouze na základě znalosti klíče. Problematika jednosměrných funkcí je podrobněji popsána například v [12].

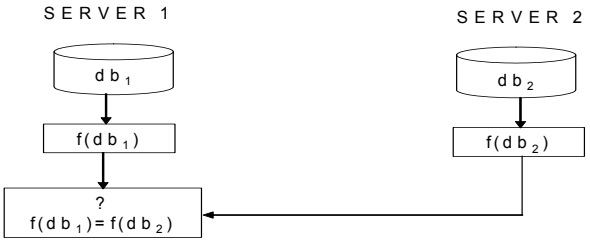
Hašovací funkce

Speciálním případem jednosměrných funkcí jsou funkce hašovací (anglicky hash function), u nichž hodnota $f(x)$ má vždy pevnou délku výstupu, obvykle několik bajtů (anglicky byte). Při nepatrné změně vstupního souboru x je změněna i výstupní hodnota $f(x)$. Jako „otisk“ souboru x pak slouží hodnota $f(x)$. Změna 1 bitu ve vstupním souboru x změní přibližně jednu polovinu bitů výstupního „otisku“ $f(x)$.

Hašovací funkce umožňují provádět kontrolu, zda nedošlo k modifikaci souboru x. Kontrola se provádí na základě porovnání již existujícího „otisku“ $f(x)$ s nově vytvořeným „otiskem“. Nemusí však jít pouze o kontrolu jednotlivých souborů, ale například o celou databázi.

Uvažujme případ, kdy pořízené záznamy organizace o transakcích s klienty jsou ukládány do rozsáhlé databáze db_1 na serveru S_1 a on-line zálohovány do databáze db_2 uložené na geograficky vzdáleném serveru S_2. V pravidelných časových intervalech

je přitom zapotřebí zkontrolovat shodnost databází. Proto se přeruší zápisy do db_1 i db_2 a databáze se uvedou do klidového stavu. Místo složitého přenášení například databáze db_2 na pracoviště s databází db_1 a jejich porovnávání se může na obě databáze aplikovat hašovací funkce f. Hodnota $f(db_2)$ se zašle na pracoviště s databází db_1 a následně se porovnají hodnoty $f(db_1)$ a $f(db_2)$. Pokud $f(db_1) = f(db_2)$, jsou s pravděpodobností prakticky rovnou 1 (viz dále) obě databáze shodné (viz obr. 1).



Obr. 1. Ověření shodnosti geograficky vzdálených databází.

Další užívanou aplikací hašovacích funkcí je i možnost ukládat uživatelská hesla v počítačových systémech. V systému není uloženo heslo, ale hodnota hašovací funkce $f(x)$, aby nedošlo k případnému zneužití hesla. Při autentizaci uživatel zadá do systému své heslo x, je vypočten „otisk“ $f(x)$ a porovnán s otiskem uloženým v systému. Pokud jsou oba „otisky“ shodné, bylo s pravděpodobností prakticky rovnou 1 zadáno správné heslo a uživateli je umožněn přístup do systému.

Hašovací funkce se může také použít k pozdějšímu prokázání autorství dokumentu x, aniž byl z nějakého důvodu zveřejněn. Stačí, pokud je uveřejněna hodnota $f(x)$. Kdykoliv je pak možné předložit dodatečně dokument x k ověření, že publikovaný „otisk“ $f(x)$ náleží souboru x. Například autor závěti zapsané v elektronické formě může zveřejnit pouze odpovídající „otisk“. Po úmrtí autora a zveřejnění závěti může kdokoliv ověřit, že nejde o podvržený nebo dodatečně upravený elektronický dokument.

Mezi běžně užívané hašovací funkce patří například SHA1 (s výstupem 20 bajtů), která je podrobně popsána v [8]. Uveďme příklad početní náročnosti získání souboru x, jehož „otisk“ je roven zadané hodnotě h (tj. $f(x) = h$). Předpokládejme, že x budeme vybírat pouze ze souborů délky 16 bajtů (128 bitů), uvažujme hašovací funkci s délkou výstupu také 16 bajtů a předpokládejme, že k získání hledaného souboru x bude zapotřebí 2^{127} pokusů. Pak při rychlosti 10^6 pokusů/s by k provedení uvedeného počtu pokusů bylo zapotřebí cca $5{,}4 \cdot 10^{24}$ let (což je více, než je současné stáří vesmíru).

Klíčované hašovací funkce

Kontrolní součty (samodetekující kódy, samoopravující kódy — viz [7]) umožňují nalézt a případně odstranit neúmyslné chyby, poruchy při přenosu dat apod. Neumožňují však zjistit, zdali nebyla vhodnou úpravou provedena neoprávněná změna souboru. Klíčované hašovací funkce užívají jako vstupní hodnotu soubor x a navíc klíč k, který zná pouze pořizovatel výstupní hodnoty $f_k(x)$ a subjekt ověřující správnost hodnoty

$f_k(x)$. Pokud by neoprávněnou změnu obsahu souboru x provedl subjekt, který nezná klíč k, nebude schopen vypočítat novou správnou hodnotu $f_k(x)$ odpovídající upravenému souboru. Klíčované hašovací funkce tak umožňují zajistit autentičnost zprávy.

2.2. Šifrovací algoritmy

Princip šifrovacího algoritmu spočívá v transformaci E textu x v čitelném tvaru (otevřený text) do nečitelného tvaru c (zašifrovaný text) a v inverzní transformaci D textu c na původní čitelný tvar x (značení E a D je převzato z anglických slov encryption a decryption). Při transformaci oběma směry se využívá tajná informace — šifrovací klíč k, bez jejíž znalosti nelze transformace realizovat. Šifrovací algoritmy umožňují redukovat správu velkých objemů dat na správu klíčů.

Mnohdy dochází mylně ke ztotožňování pojmů *šifrování* a *kódování*. Základní rozdíl spočívá v tom, že při zašifrování se využívá tajná informace (klíč k) a bez její znalosti nelze získat ze zašifrovaného souboru žádnou informaci. Naproti tomu kódování je transformace jedné formy zápisu informace do jiné formy, která je z nějakého důvodu pro danou situaci výhodnější (například ASCII kódy, čárové kódy výrobků). Přitom obě formy zápisu jsou veřejně přístupné.

Z pohledu postupu zašifrování otevřeného textu lze moderní šifry rozdělit zhruba do dvou základních skupin.

První tvoří algoritmy s *proudovým šifrováním*, kdy se šifruje po bitech/bajtech. Přitom v každém kroku šifrování může docházet k modifikaci šifrovacího klíče (například algoritmy RC4, A5 popsané v [12]).

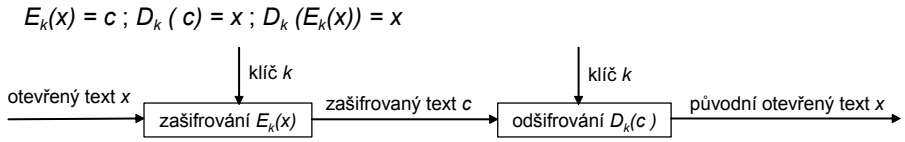
Druhou skupinu tvoří *algoritmy s blokovým šifrováním*, které šifrují více bajtů najednou. Blok otevřeného textu vstupuje do algoritmu, výstupem je blok stejné délky zašifrovaného textu (například metoda DES popsaná v [8] šifruje bloky délky 8 bajtů).

Z hlediska užití šifrovacího klíče k rozlišujeme následující dvě základní skupiny algoritmů.

Symetrické šifrování

Algoritmy se symetrickým šifrováním realizují transformace zašifrování E_k i odšifrování D_k užitím stejného tajného klíče k[1]), kdy odesílatel i příjemce zašifrované zprávy užijí tentýž klíč (viz obr. 2). Před vlastním použitím symetrického algoritmu musí být zajištěna distribuce tajného klíče k všem stanoveným účastníkům komunikace pomocí důvěrného kanálu.

[1]) Algoritmy se symetrickým šifrováním obecně realizují transformace zašifrování pomocí tajného klíče k_1 a odšifrování užitím tajného klíče k_2. Přitom v každém příslušném páru klíčů k_1, k_2 lze početně snadno určit k_2 ze znalosti k_1 a naopak. U většiny v současnosti užívaných algoritmů se symetrickým šifrováním platí $k_1 = k_2$, kdy odesílatel i příjemce zašifrované zprávy užijí tentýž klíč k.



Obr. 2. Symetrické šifrování.

Příkladem symetrického šifrování je *jednorázová šifra*. Klíč k je stejné délky jako otevřený text x (tj. má stejný počet bitů). Při šifrování se užívá binární logická operace xor, která je definována takto:

$$\begin{aligned} 0 \text{ xor } 0 &= 0, \\ 1 \text{ xor } 0 &= 1, \\ 0 \text{ xor } 1 &= 1, \\ 1 \text{ xor } 1 &= 0. \end{aligned}$$

Z uvedené definice vyplývá, že $a \text{ xor } a = 0$, a tedy $a \text{ xor } b \text{ xor } b = a$ pro libovolné $a, b \in \{0, 1\}$. Šifrovaný text je dán vztahem

$$c(i) = x(i) \text{ xor } k(i) \quad \text{pro } i = 1, \ldots, n, \tag{2.2}$$

kde n udává počet bitů otevřeného textu x. Šifruje se postupně bit po bitu celý otevřený text x za použití klíče k. Klíč k je vytvořen (pseudo)náhodným generátorem 0 a 1 a po jednom použití se ničí, aby byla zajištěna absolutní bezpečnost šifry. Příjemce po obdržení zašifrovaného textu c provede odšifrování

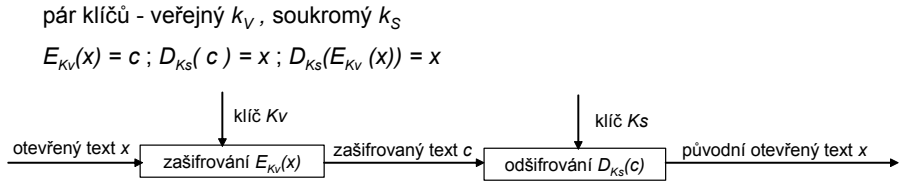
$$x(i) = c(i) \text{ xor } k(i) \quad \text{pro } i = 1, \ldots, n. \tag{2.3}$$

V praxi jsou generovány sady klíčů (posloupností 0 a 1), které jsou důvěrnou cestou předány budoucímu příjemci zpráv. Jednorázová šifra se správně generovaným klíčem je absolutně bezpečná, neboť zašifrovaný text c nenese žádnou informaci o otevřeném textu x. Užívá se zejména k zajištění důvěrnosti důležitých informací v diplomatických kruzích, kdy je nutné zaručit maximální bezpečnost.

Užívanými symetrickými algoritmy jsou například DES (s délkou symetrického klíče 56 bitů), upravený algoritmus DES nazývaný Triple DES (112, resp. 168 bitů), IDEA (128 bitů), AES (128, 176, resp. 256 bitů). Uvedené algoritmy jsou popsány v [8], algoritmus AES v [5].

Asymetrické šifrování

Algoritmy asymetrického šifrování jsou založeny na principu jednosměrných funkcí s „padacími vrátky“. Algoritmy užívají pár klíčů — klíč veřejný k_V a klíč soukromý k_S. Oba klíče jsou spolu jednoznačně svázány. Veřejný klíč k_V je volně dostupný, v tajnosti drží vlastník páru klíčů pouze svůj soukromý klíč k_S. Ze znalosti veřejného klíče k_V



Obr. 3. Asymetrické šifrování.

je technicky velmi obtížné zjistit soukromý klíč k_S. K zašifrování otevřeného textu x může kdokoliv užít veřejný klíč k_V adresáta. Odšifrovat text c však může pouze adresát — vlastník páru klíčů za použití svého soukromého klíče k_S (viz obr. 3).

V roce 1978 byl publikován algoritmus asymetrického šifrování RSA (autorů Rivesta, Shamira a Adlemana), který stále patří mezi nejužívanější algoritmy (viz [11]). Princip metody je založen na jednoduchém výpočtu hodnoty $n = p \cdot q$, kde p a q jsou prvočísla obsahující 100 až 200 nebo i více cifer. Při neznalosti obou prvočísel je však technicky prakticky nerealizovatelné provést faktorizaci hodnoty n. U této metody je veřejný klíč dán dvojicí hodnot $k_v = [e, n]$ a odpovídající soukromý klíč dvojicí hodnot $k_s = [d, n]$. Dvojice celočíselných hodnot e a d je jednoznačně určena, ale ze znalosti e a n je technicky obtížné určit hodnotu d, která je součástí soukromého klíče. Při šifrování metodou RSA v praxi se užívají klíče délky 512, 1024, resp. 2048 bitů (tj. počet bitů užitých k vyjádření hodnoty n).

Pro výměnu klíčů mezi komunikujícími stranami se používá například algoritmus DH (Diffie-Hellman), založený na složitosti výpočtu diskrétního logaritmu. Podrobně jsou uvedené metody popsány v [12].

Šifrování pomocí asymetrických šifer je velice náročné na počet operací v porovnání s použitím symetrických systémů. Například hardwarová realizace metody RSA je cca 1000krát pomalejší při šifrování než DES a softwarová cca 100krát pomalejší. Proto se asymetrické šifry používají především k distribuci klíčů symetrických šifer, k digitálnímu podpisu (viz dále) a k dalším speciálním účelům (například distribuce inicializačních hesel, PINů). Symetrické šifry jsou využívány především k šifrování souborů.

Existují také *hybridní algoritmy*, u nichž se k šifrování používá symetrická šifra s jednorázovým klíčem k, který je zašifrován veřejným klíčem k_V adresáta užitím asymetrické šifry. K zašifrovanému textu c se přiloží zašifrovaný klíč k symetrické šifry a text se zašle příjemci.

2.3. Digitální podpis

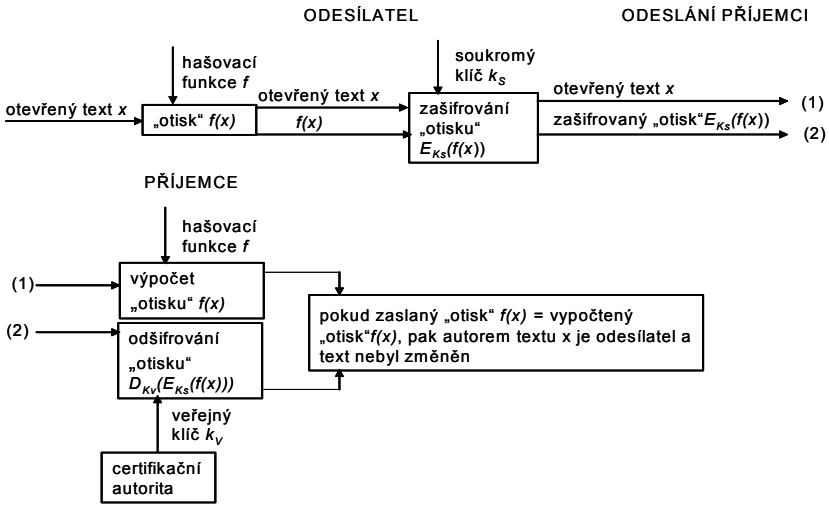
Užívá se k ověření, že text x pochází skutečně od odesílatele (zajištění autentičnosti a principu neodmítnutelnosti) a že původní obsah nebyl změněn. Jedna z variant digitálního podpisu je založena na následujícím principu. Na otevřený text x aplikuje odesílatel hašovací funkci f a obdrží „otisk“ $f(x)$ otevřeného textu x, $f(x)$ je pevné délky několika bajtů. „Otisk“ $f(x)$ pak zašifruje odesílatel svým soukromým klíčem k_S

algoritmu asymetrického šifrování — vytvoří digitální podpis textu x. Zašifrovaný „otisk“ zašle společně s otevřeným textem x příjemci. Příjemce po obdržení zprávy aplikuje stejnou hašovací funkci f na doručený otevřený text x. Současně odšifruje veřejným klíčem odesílatele zašifrovaný „otisk“ $f(x)$. Pokud se odšifrovaný „otisk“ shoduje s vypočteným „otiskem“ $f(x)$, je zpráva původní a nebyla modifikována.

Veřejné klíče algoritmů asymetrického šifrování spravuje instituce zvaná certifikační autorita (CA). Jejím hlavním posláním je garantovat pravost a platnost veřejného klíče vlastníka páru klíčů. Na obr. 4 je znázorněn princip digitálního podpisu a jeho ověření.

Pokud je digitálně podepsaný otevřený text x důvěrného charakteru, může být před odesláním společně s digitálním podpisem zašifrován.

V současnosti se používá pro digitální podpis například algoritmus DSA (viz [12]).

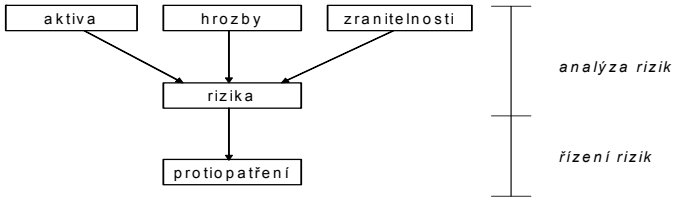


Obr. 4. Schéma vytvoření a ověření pravosti digitálního podpisu.

3. Realizace zabezpečení informací

Aby prostředky na zabezpečení byly vynaloženy efektivně, je nezbytné řešit uvedený problém komplexně a realizovat bezpečnostní opatření ve všech potřebných oblastech a ve vzájemné součinnosti. Často se v praxi stává, že specialisté v jednotlivých oblastech zabezpečení informací si dostatečně neuvědomují potřebu komplexně řešit zabezpečení IS nebo nezbytnost bezpečnostních opatření ve zbývajících oblastech podceňují.

Abychom byli schopni stanovit přiměřená bezpečnostní opatření pro daný IS, potřebujeme nejdříve získat následující údaje (přesněji odhady údajů): ocenění (důležitost) existujících informací pro organizaci a ocenění dalších aktiv IS, znát potenciální hrozby a jejich závažnost pro jednotlivá aktiva, zranitelnost aktiv vůči těmto hrozbám (viz obr. 5).



Obr. 5. Složky podílející se na stanovení bezpečnostních opatření.

Hrozby pocházejí především z oblasti nedovolených aktivit uživatelů, správců IS a cizích osob, technických a programových závad (úmyslných i neúmyslných), teroristických akcí a přírodních živlů.

Jiným možným přístupem k zabezpečení IS je realizace základních bezpečnostních opatření doporučených některými metodikami, aniž je provedena analýza rizik. Tento postup však nezajistí minimalizaci existujících rizik.

3.1. Ocenění aktiv IS

Ocenění informací je obtížný a specifický krok pro každou organizaci. Vedoucí pracovníci často požadují stanovení významu informací pomocí finančního vyjádření. Pro potřeby bezpečnosti však tento přístup není příliš vhodný a často vede k chybným závěrům.

Popišme stručně jeden z možných a v praxi ověřených přístupů. Užívá se v některých kvantitativních metodách analýzy rizik, například v metodologii CRAMM (CCTA Risk Analysis and Management Method), která je podrobněji popsána v [2].

Před vlastním oceněním informací je zapotřebí provést v organizaci jejich identifikaci. Informace jsou obvykle seskupovány do větších celků — informačních jednotek (například informace o klientech obchodní společnosti, informace o zaměstnancích, strategické záměry a plány).

Ocenění informací je založeno na principu odhadu nejhorších možných dopadů pro společnost, které lze očekávat v následujících třech případech:

- *informace je vyzrazena a zneužita* (například konkurenční společností),
- *modifikace informace* (modifikace záměrná neoprávněná nebo v důsledku chyby),
- *nedostupnost informace* (po nějaký časový interval nebo zničení bez možnosti její obnovy).

Vhodně vybraný respondent ve spolupráci se specialisty na analýzu rizik IS odhaduje možné negativní dopady pro uvedené 3 případy. Za oblast negativního dopadu bývá například považována „ztráta dobrého jména organizace“, „narušení řízení a provozu organizace“, „poškození ekonomických a obchodních zájmů organizace“, „nedodržení právních a regulatorních závazků“, „finanční ztráty“, „ohrožení personální bezpečnosti“. Uvažované oblasti negativního dopadu přirozeně závisí na specifikách dané organizace. Každá oblast se ještě podle závažnosti dopadu dělí do několika úrovní

a jednotlivým úrovním je přidělena celočíselná hodnota mezi 1 až M. Maximální obdržená hodnota ze všech oblastí dopadu pak udává ocenění informační jednotky.

Každou informační jednotku je zapotřebí ohodnotit ze všech tří uvažovaných pohledů.

Možné negativní důsledky se mohou zkoumat pro každé hledisko podrobněji (například negativní dopady nedostupnosti informační jednotky pro různé časové intervaly).

Ocenění informací je vždy ovlivněno subjektivním pohledem respondenta, proto je zapotřebí provádět pečlivě jejich výběr.

Softwarová aktiva lze ocenit obdobně jako informační jednotky, cena hardwarových aktiv odpovídá pořizovací ceně nového adekvátního zařízení. U softwarových a hardwarových aktiv však je ještě zapotřebí uvažovat přidanou hodnotu v závislosti na tom, jak důležitou informační jednotku podporují.

3.2. Stanovení míry rizika

Jednotlivým aktivům IS lze přiřadit hrozby na základě doporučení použité metodiky, vlastních zkušeností specialisty analýzy rizik IS a konkrétních podmínek v daném IS. Míru rizika m pro konkrétní dvojici aktivum–hrozba lze stanovit jako hodnotu funkce g tří proměnných dané vztahem

$$m = g(v, x, y), \tag{3.1}$$

kde v je ocenění aktiva, x závažnost hrozby, y stupeň zranitelnosti aktiva vůči hrozbě. Hodnotu x a y lze obdržet na základě interview se správci a pracovníky podpory. V praktických metodikách se rozlišuje několik stupňů závažnosti hrozby (například velmi nízká, nízká, střední, vysoká, velmi vysoká) a několik stupňů zranitelnosti aktiva (například nízká, střední, vysoká), v nabývá jako v předchozím odstavci celočíselné hodnoty 1 až M. Funkce g je pak zadána pomocí třídimenzionální matice, jejíž prvky reprezentují hodnotu míry rizika m (obvykle nabývá celočíselné hodnoty 1 až N) v závislosti na ocenění aktiva v, stupně závažnosti hrozby x a stupně zranitelnosti y.

Cílem analýzy rizik není úplná eliminace rizika, ale snížení míry rizika realizací bezpečnostních opatření na přijatelnou úroveň pro organizaci (tzv. zbytkové riziko).

3.3. Bezpečnostní opatření

Po analýze rizik IS je zapotřebí realizovat bezpečnostní opatření.

Základní dokument řešící koncepčně informační bezpečnost v organizaci se obvykle nazývá *Bezpečnostní politika IS*. Jeho podrobnější a konkretizované rozpracování pro jednotlivé subsystémy bývá realizováno v dokumentech nazývaných *Systémová bezpečnostní politika IS* (problematika bezpečnostních politik je podrobně řešena v [15] a [16]).

Úroveň bezpečnostního opatření je přiřazena v závislosti na míře rizika m dvojice aktivum–hrozba.

Bezpečnostní opatření se realizují v oblastech fyzických komponent IS (hardware), programového vybavení, řízení, procedurální a personální.

4. Závěr

Zabezpečení elektronických informací se stává součástí aktivit každé organizace. Ne všechny však realizují informační bezpečnost efektivně a komplexně.

Často se v organizacích aplikují bezpečnostní opatření bez znalosti (odhadu) míry existujících rizik v IS. Takový přístup však vede většinou ke slabým místům zabezpečení (a organizace o nich často vůbec netuší) a k neefektivnímu vynakládání prostředků.

V důsledku nepřetržitého vývoje každé organizace a rozvoje výpočetní techniky dochází průběžně i ke změnám v IS organizace. Zabezpečení IS každé organizace je proto kontinuální a nekončící proces.

Kromě již uvedených odkazů na literaturu odkazuji zájemce o analýzu a řízení rizik na [14], kryptografii jsou věnovány publikace [4] a [10], právní otázky spojené s digitálním podpisem se řeší v [1], specifiky bankovní bezpečnosti se zabývá [13] a zabezpečením elektronických informací obchodních společností [9]. Norma [3] se v současnosti považuje v mezinárodním měřítku za výchozí materiál pro realizaci komplexní bezpečnosti IS.

Literatura

[1] Bosáková, D. a kol.: *Elektronický podpis.* Grada, Praha 2002.
[2] CRAMM: `http://www.cramm.com`
[3] ČSN/ISO/IEC 17799:2000 Code of Practice for Information Security Management.
[4] Grošek, O., Porubský, Š.: *Šifrovanie — algoritmy, metódy, prax.* Grada, Praha 1992.
[5] Klíma, V.: *AES — nová šifra nastupuje.* Chip, květen 2002, 142–144.
[6] Křížek, M., Luca, F., Somer, L.: *17 Lectures on Fermat Numbers.* Springer-Verlag, New York 2001.
[7] Křížek, M., Šolcová, A.: *Prvočíslo* 11 *v kódování.* Rozhledy mat.-fyz., ročník *78* (2004), 208–204.
[8] Menezes, A., Oorschot, P., Vanstone, S.: *Handbook of Applied Cryptography.* CRC Press, LLC, 2000 N. W. Corporate Blvd., Boca Raton, Florida 2001.
[9] Mlýnek, J.: *Zabezpečení obchodních informací.* TUL Liberec 2006 (v tisku).
[10] Přibyl, J.: *Informační bezpečnost a utajování zpráv.* ČVUT, fakulta elektrotechnická, vydavatelství ČVUT, Praha 2004.
[11] Rivest, R. L., Shamir, A., Adleman, L. M.: *A Method for Obtaining Digital Signatures and Public Key Cryptosystems.* Communications of the ACM, v. 21, n. 2, pp. 120–126, Feb 1978.
[12] Schneier, B.: *Applied Cryptography.* John Wiley & sons, New York 1996.
[13] Sloupenský, V., Žehra, F.: *Bankovní bezpečnost.* Bankovní institut, Praha 1997.
[14] Smejkal, V., Rais, K.: *Řízení rizik.* Grada, Praha 2003.
[15] Wood, Ch.: *Information Security Policies Made Easy.* Information Shield, Inc., Bering, Houston 2005.
[16] Wood, Ch.: *Information Security Roles and Responsibilities Made Easy.* Information Shield, Inc., Bering, Houston 2005.