# RIADENIE RIZÍK OPERAČNÉHO SYSTÉMU

**Masár Juraj**
*Katedra informatiky a počítačů, Přírodovědecká fakulta, Ostravská univerzita v Ostravě, 30. dubna 22, 701 03 Ostrava, 597 092 100, juraj.masar@osu.cz*

**Abstrakt**

Dnešné organizácie majú čoraz väčšie nároky na informačnú bezpečnosť. Mnoho z nich však nemá vytvorenú bezpečnostnú politiku, ktorá sa vzťahuje na operačné systémy. Administrátori tak využívajú počas implementácie jednotlivých ochranných opatrení poznatky z neformálnej analýzy rizík, čo môže viesť v niektorých prípadoch k oslabeniu alebo úplnému zlyhaniu bezpečnosti daného systému, pretože nevyužívajú systémový prístup. Našim cieľom je vytvorenie modelu, ktorý bude popisovať riadenie rizík operačného systému vychádzajúce z podrobnej analýzy rizík. Model formalizujeme pomocou Petriho siete v aplikácii HPSim, pričom na jeho zostavenie využijeme existenciu metodiky, ktorá sa týka manažmentu rizík IT uvedeného v medzinárodnej norme ISO/IEC.

***Kľúčové slová:*** *Operačný systém; model bezpečnosti; riadenie rizík; aktíva; hrozba.*

## Úvod

Informácie, rôzne podporné procesy, systémové zdroje a siete patria medzi najkritickejšie aktíva nejednej organizácie. S postupným rozvojom sa organizácia stáva čoraz viac závislejšia od svojich aktív a tie sú častejšie vystavované bezpečnostným hrozbám, ktoré pochádzajú z rôznych zdrojov a spôsobujú škody, čím znižujú jej konkurencieschopnosť.

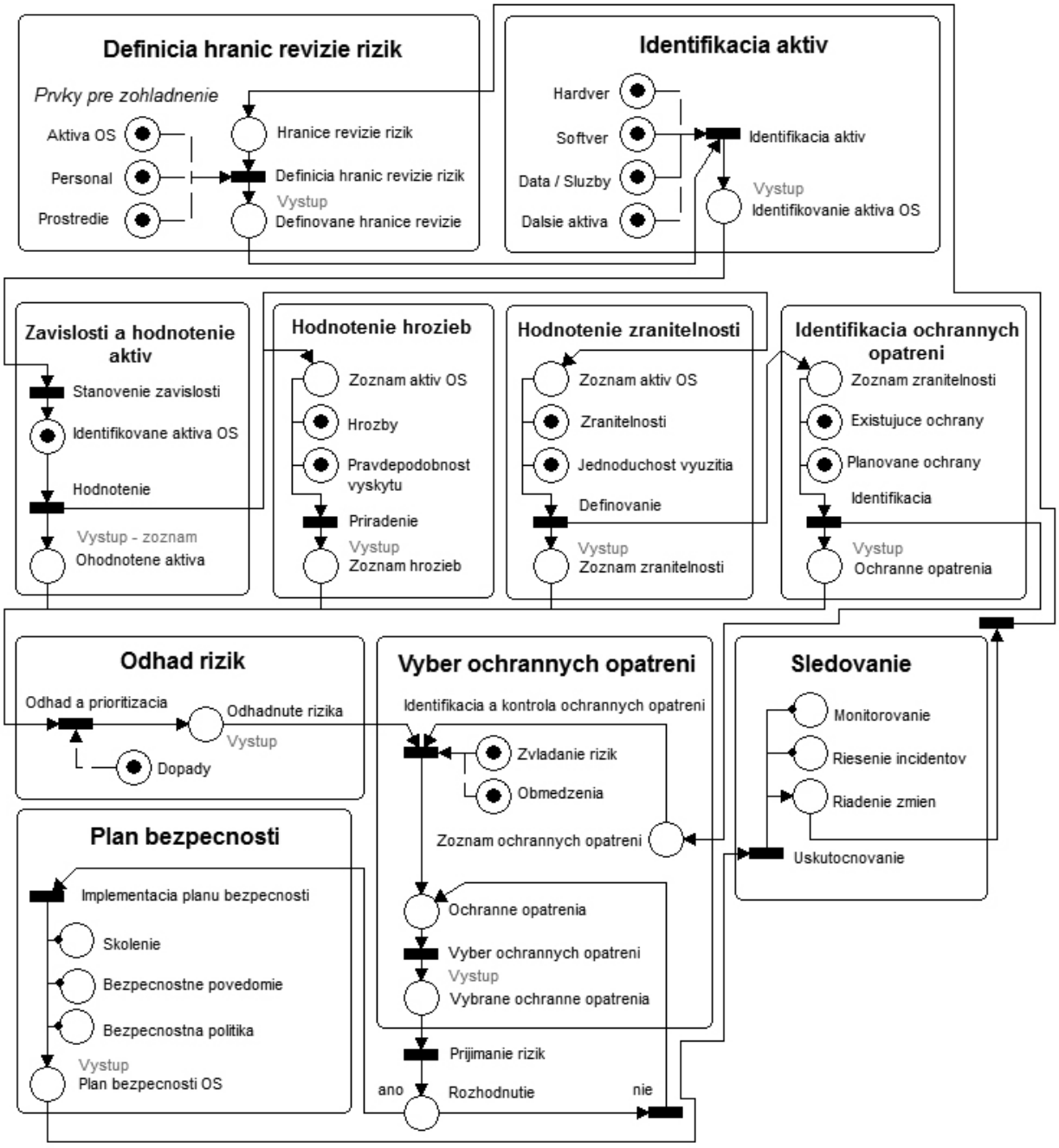
Úloha operačného systému spočíva v zabezpečení dostupnosti a manažmentu týchto aktív. Z tohto dôvodu by mali byť pre jeho ochranu prijaté a implementované adekvátne bezpečnostné opatrenia, aby sa minimalizovalo riziko narušenia informačnej bezpečnosti aktív, t.j. narušenie ich dôvernosti, integrity a dostupnosti. So stúpajúcimi nárokmi na informačnú bezpečnosť a tiež zvyšujúcou sa komplexnosťou dnešných operačných systémov je potrebný pre vhodnú a zároveň efektívnu selekciu bezpečnostných opatrení, najmä z časových a finančných nákladov, systémový prístup.

## Riadenie informačných rizík

Manažment informačných rizík predstavuje komplexný a cyklický proces, ktorý sa skladá z niekoľkých na seba nadväzujúcich fáz. Cieľom tohto procesu je identifikovanie, eliminovanie alebo minimalizovanie a následná kontrola udalostí, ktoré môžu negatívne ovplyvniť bezpečnosť systému, pričom celý proces by mal byť prijateľný z časového a finančného hľadiska. [1]

Riadenie rizík operačného systému bude v našom prípade pozostávať z fázy definovania hraníc revízie bezpečnostných rizík, analýzy rizík a ich odhadu, výberu príslušných ochranných opatrení s prihliadnutím na určité obmedzenia, akceptovania reziduálnych rizík, implementácie bezpečnostného plánu a posledná fáza sa bude týkať sledovania rizík.

Proces riadenia rizík OS, ktorý je zobrazený na nasledujúcej ilustrácii (Obr. 1), formálne vyjadríme prostredníctvom modelu Petriho siete definovanej ako $N = (P,T,F)$, kde $P$ predstavuje množinu miest (Places) siete $N$, $T$ predstavuje množinu prechodov (Transitions) a $F$ predstavuje tokovú reláciu (Flow relation) siete $N$, pričom procesy vykonávané v jednotlivých fázach riadenia rizík budú reprezentované pomocou prechodov a k nim pridružené vstupy pomocou miest. [2]




Obr.1 Proces riadenia rizík OS (čiastočne založený na ISO/IEC TR 13335-3)

**Definícia hraníc revízie rizík**

Ešte pred samotným uskutočnením analýzy rizík OS by sme mali stanoviť hranice revízie v rámci ktorých budeme uvažovať o bezpečnostných rizikách, pretože ich dôsledným stanovením je možné znížiť čas a zvýšiť kvalitu analýzy rizík. Popis týchto hraníc by mal jednoznačne určiť aké prvky by sme mali v rámci analýzy rizík zohľadniť. Príkladom týchto prvkov sú aktíva OS (informácie, softvér, hardvér, dokumentácia), personál (používatelia, administrátori, zamestnanci) alebo prostredie (umiestnenie budov, elektrické napájanie, klimatizácia), prípadne komunikácia v počítačovej sieti. Vymedzenie hraníc revízie môže ovplyvniť aj bezpečnostná politika. [3]

**Analýza rizík**

Podrobná analýza rizík operačného systému bude pozostávať z viacerých krokov, v ktorých identifikujeme a ohodnotíme jeho aktíva, hrozby, zraniteľnosti a ochranné opatrenia. Výsledky týchto krokov budú predstavovať vstup pre odhad rizík operačného systému.

*Identifikácia a hodnotenie aktív* zahŕňa identifikovanie všetkých aktív OS a ich vzájomných vzťahov spadajúcich do nami stanovených hraníc revízie. Následne im priradíme hodnoty, ktoré reprezentujú ich význam z pohľadu činnosti organizácie v súvislosti s narušením ich bezpečnosti, pričom toto hodnotenie môže byť v kvantitatívnom alebo kvalitatívnom meradle. Vstupné údaje pre hodnotenie by nám mali poskytnúť správcovia OS a bezpečnostná politika organizácie.

*Identifikácia a hodnotenie hrozieb* zahŕňa identifikáciu zdrojov a pravdepodobností výskytu bezpečnostných hrozieb, ktorým sú vystavené uvažované aktíva OS. Vstupné údaje pre odhad hrozieb je možné získať od správcov OS, špecialistov na bezpečnosť, dokumentácie, technických noriem, prípadne všeobecných alebo špecifických katalógov popisujúcich hrozby. Pre vyjadrenie pravdepodobnosti ich výskytu použijeme kvalitatívne hodnotenie, t.j. stupnicu s hodnotami malý, stredný, vysoký, pričom budeme brať do úvahy štatistický počet výskytov, motiváciu útočníka a faktory prostredia. Výstupom bude zoznam aktív spolu s hrozbami, ktorým sú vystavené a tiež s pravdepodobnosťou výskytu týchto hrozieb.

*Identifikácia a hodnotenie zraniteľností* predstavuje odhad slabých miest, ktoré majú aktíva OS, prípadne ich vlastnosti resp. atribúty. Najčastejšie ide o zraniteľnosti vo fyzickom prostredí, hardvéru, softvéru, postupoch pri používaní alebo administrácii OS, alebo zraniteľnosti týkajúce sa komunikácie v sieti. Zraniteľnosti, ktoré nemajú zodpovedajúcu hrozbu, nepredstavujú riziko a nevyžadujú žiadne ochranné opatrenia. Vstupné údaje pre odhad zraniteľností je možné získať rovnakým spôsobom ako v predchádzajúcom prípade. Výstupom bude zoznam identifikovaných zraniteľností u príslušných aktív OS spolu s kvalitatívnym odhadom, ktorý bude vyjadrovať jednoduchosť využitia zraniteľností bezpečnostnou hrozbou.

*Identifikácia ochranných opatrení* zahŕňa identifikáciu existujúcich a taktiež plánovaných ochranných opatrení. V rámci tohto kroku dôjde ku kontrole kompatibility existujúcich prípadne plánovaných ochranných opatrení a tiež k uskutočneniu kontroly, či tieto existujúce ochranné opatrenia fungujú správne. Vo fáze výberu ochranných opatrením nám tento krok zmenší časové a finančné náklady a bude nás chrániť pred aplikovaním viacnásobných ochranných opatrení. Výstupom je zoznam existujúcich a plánovaných ochranných opatrení.

*Odhad rizík* predstavuje posledný krok tejto fázy. Jeho cieľom je odhadnutie jednotlivých rizík pôsobiacich na operačný systém a jeho aktíva, na základe ktorých dôjde k výberu vhodných ochranných opatrení. Bezpečnostné riziko je charakterizované ako funkcia, v ktorej vystupuje hodnota aktíva, pravdepodobnosť výskytu hrozby spôsobujúcej nepriaznivý dopad, jednoduchosť využitia zraniteľnosti danou hrozbou a identifikované ochranné opatrenie znižujúce riziko. Pre meranie týchto vzťahov je možné použiť viacero metód, ktorých výstupom bývajú matice alebo tabuľky rizík. Výstupom tohto kroku bude zoznam nameraných rizík pôsobiacich na aktíva OS v kontexte s narušením integrity, dôvernosti a dostupnosti. [3]

**Výber ochranných opatrení**

Zaistenie primeranej ochrany operačného systému uskutočníme na základe intenzity rizík, ktoré sme stanovili v predchádzajúcej fáze. Aby sme znížili riziká na prijateľnú úroveň, môžeme selektovať ochranné opatrenia tak, že sa vo všeobecnosti rizikám vyhneme, presunieme ich, alebo zredukujeme hrozby a zraniteľnosti, znížime dopady, prípadne zabezpečíme detekciu incidentov a zotavenie sa z nich. Pri identifikácii ochranných opatrení je však užitočné, aby sme zohľadnili zraniteľnosti a hrozby, ktoré ich využívajú, existenciu alternatívnych ochranných opatrení a tiež

existenciu rôznych obmedzení (časové, finančné, technické, atď.). Súčasťou tejto fázy je ešte proces rozhodnutia, či je úroveň bezpečnosti prijateľná a akceptovaniu zvyškových rizík, ktoré budú podliehať následnému monitorovaniu. [3]

**Bezpečnostný plán**

Počas tejto fázy dochádza k implementácii vybraných ochranných opatrení. Pri všetkých ochranných opatreniach je potrebné, aby boli riadne zdokumentované, vrátane ich konfigurácie a tiež informácií o aktívach, ich uložení, sprístupňovaní a používaní. Taktiež je potrebné vytvoriť havarijné plány, vymedziť zodpovednosti, zvyšovať bezpečnostné povedomie pomocou školení a vytvorenie resp. aktualizovanie bezpečnostnej politiky. [3]

**Sledovanie**

Táto fáza pozostáva z detekcie a riešenia incidentov, riadenia zmien, monitorovania rizík, sledovania stavu aktív a ich dostupnosti v závislosti na čase, vykonávania aktualizácií a revízií ochranných opatrení a aktív, spracovávania auditných záznamov a podobne. [3]

**Záver**

Uvedený model riadenia bezpečnostných rizík je možné aplikovať na akýkoľvek operačný systém a tým zaistiť požadovanú úroveň bezpečnosti pre jeho aktíva. Využíva podrobnú analýzu rizík, ktorá však môže byť v niektorých prípadoch pre výber adekvátnych ochranných opatrení v porovnaní so základnou analýzou rizík a výberom štandardných ochranných opatrení zbytočne časovo a finančne nákladná. Preto odporúčame aplikáciu tohto modelu iba pre operačné systémy s kritickými aktívami.

Predmetom ďalšieho výskumu bude detailnejšie rozpracovanie tohto modelu a jeho vzťahu, s riadením zraniteľností, aktualizácií a zmien a tiež riešenie výberu vhodnej metódy slúžiacej pre odhad rizík vrátane porovnania už s existujúcimi metodikami, ktoré sa zaoberajú riadením rizík. Nasledovné výstupy bude možné uplatniť v rámci projektu SGS pri tvorbe fuzzy modelovacieho nástroja pre testovanie a návrh informačných systémov.

**Literatúra**

[1.] ČSN ISO/IEC TR 13335-1 - Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT. Praha: Český normalizační institut, 1999. 24 s. EAN: 8590963560946

[2.] REISIG, W. Petri Nets: An Introduction. Germany: Springer, 1985. 161 s. ISBN 978-0387137230

[3.] ČSN ISO/IEC TR 13335-3 - Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT. Praha: Český normalizační institut, 2000. 48 s. EAN: 8590963583723

**Abstract**

Today's organizations are increasing requests to information security. Many of them have not created a security policy related to operating systems. Their administrators use knowledge of informal risk analysis in the implementation process of safeguards, which may lead in some cases to a reduction or complete failure of the system security, because they don't use a systematic approach. Our goal is to create a model of the operating system risk management process based on detailed risk analysis, which will be formalized by Petri nets in the application called HPSim. The model will be based on existing methodology of the IT risk management, which was introduced in the technical report of ISO/IEC standards.