Bezpečnost informačních systémů a jejich kvalita

Marek Čandík

Policejní akademie České republiky v Praze

Vlastnosti informačního systému je možné charakterizovat jeho charakteristikami jakosti (quality characteristics). Jakost je chápána jako míra splnění požadavků uživatele. Významným atributem informačních systémů je software. Tento produkt je zbožím se specifickými vlastnostmi, ze kterých lze uvést:

- Je nehmotný, a proto jeho jakost nelze změřit jinak než porovnáním, nakolik jsou splněny cíle očekávané uživatelem.
- Uživatel není schopen kritéria pro hodnocení jakosti programu dostatečně přesně specifikovat.
- Požadavky na program se velmi rychle mění, mnohdy i v průběhu jeho tvorby.
- Tvorba programu je velmi složitý proces, a proto je vysoká pravděpodobnost že se zde objeví neshody (chyby), rovněž software je složitým díky několika milionům mikroprocesorových instrukcí, proto je jeho vyhodnocení obtížné.

Mezi charakteristiky informačních systémů (včetně softwarových produktů) patří:

- Funkčnost (functionality) - Funkčnost je vymezená jako schopnost informačního systému (respektive softwarového produktu) obsahovat funkce, které zabezpečují předpokládané nebo stanovené potřeby uživatele při používání systému za stanovených podmínek. Tato charakteristika zjišťuje, zdali jsou funkce informačního systému zabezpečené, nehovoří o tom, jak jsou zabezpečené. Funkčnost informačního systému (softwarového produktu) zahrnuje tyto atributy (podcharakteristiky):
    - Funkční přiměřenost (suitability). Funkční přiměřenost je vymezená jako schopnost informačního systému (softwarového produktu) poskytovat funkce pro zajištění blíže specifikovaných úloh a cílů uživatele.
    - Přesnost (accuracy). Přesnost je vymezená jako schopnost informačního systému (softwarového produktu) poskytnout správné a požadované výsledky s potřebnou úrovní přesnosti.
    - Schopnost spolupráce (interoperability). Schopnost spolupráce je vymezená jako schopnost informačního systému (softwarového produktu) spolupracovat s jedním či vícero jinými specifikovatelnými systémy
    - Bezpečnost (security). Bezpečnost je vymezená jakožto schopnost informačního systému (softwarového produktu) chránit informace a data tak, aby neautorizovaná osoba nebo systém neměly možnost přečíst si je, či je modifikovat a přitom aby autorizovaným subjektům nebyla zamítnuta možnost přístupu k datům na stanovené úrovni
    - Shoda ve funkčnosti (functionality compiliance). Shoda ve funkčnosti se charakterizuje jako schopnost informačního systému (softwarového produktu)

pracovat ve shodě s normami, standardy, zákony, konvencemi a zvyklostmi prostředí, ve kterém je informační systém respektive produkt využívaný.

- Bezporuchovost (relibility). Bezporuchovost je vymezená jako schopnost informačního systému (softwarového produktu) zachovat si specifickou úroveň výkonu při používání systému za stanovených podmínek. Bezporuchovost zahrnuje tyto atributy:
  - Zralost (maturity). Zralost je vymezená jako schopnost informačního systému (softwarového produktu) vyvarovat se poruchám (selháním) v důsledku závad informačního systému, nebo důsledky takovýchto závad minimalizovat. Poruchu (failure) je možné charakterizovat jako stav, kdy systém neplní svoje funkce, nebo se chová jinak, než se od něj požaduje. Porucha je většinou způsobená odchylkou funkce hardwaru, softwaru, nebo obsluhy od požadavků na informační systém. Taková odchylka stavu informačního systému od požadovaného stavu se nazývá vada, respektive závada (fault). Vada softwaru se označuje jako chyba (error).
  - Odolnost vůči vadám (fault tolerance). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) zachovat si při selhání systému, nebo při nedodržení požadovaného rozhraní ze strany uživatele určitou úroveň výkonu, respektive úroveň poskytovaných služeb.
  - Schopnost zotavení se (recoverability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) obnovit úroveň výkonu a zachovat data pro odstranění poruchy.
- Použitelnost (usability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) být srozumitelný, s lehko naučitelnou obsluhou, schopnost být atraktivní pro uživatele za stanovených podmínek. Použitelnost informačního systému (softwarového produktu) zahrnuje tyto atributy:
  - Srozumitelnost (understandability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu), která umožňuje uživateli rozhodnout, či se informační systém (softwarový produkt) hodí pro řešení jeho problémů a jak je možné ho využít pro řešení jednotlivých úloh a za jakých podmínek. Srozumitelnost je charakterizována mírou úsilí, které je potřebné k tomu, aby uživatel sám porozuměl tomu, co může od informačního systému (softwarového produktu) očekávat.
  - Naučitelnost (learnability). Tento atribut je charakterizován mírou úsilí, které je třeba vynaložit pro rutinní využívání možností informačního systému (softwarového produktu).
  - Provozuschopnost (operability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) ulehčující jeho obsluhu a řízení rutinní práce s informačním systémem (softwarovým produktem).
  - Atraktivnost (attractiveness). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) umožnit příjemnou obsluhu a přitažlivé využití informačního systému (softwarového produktu).
  - Ovladatelnost (usability compliance). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) vykonávat definované operace.

- Účinnost (efficiency). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) poskytovat potřebný výkon vzhledem k množství použitých zdrojů (například software, systémové prostředky – hardware, software) při používání za stanovených podmínek. Účinnost informačního systému (softwarového produktu) zahrnuje tyto atributy:
  - Chování v čase (time behaviour). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) zajistit požadovanou přípustnost úloh za dané časové období, čas výpočtu definovaných úloh, nebo odezvu informačního systému (softwarového produktu) při jejich používání za definovaných podmínek.
  - Využití zdrojů (resource utilisation). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) zajistit požadované funkce přiměřeným množstvím typů a množstvím a rozsahem použitelných zdrojů, které jsou potřebné k zabezpečení práce informačního systému (softwarového produktu).
  - Shoda v účinnosti (efficiency compiliance). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) produkovat požadované množství a kvalitu výstupů.
- Udržovatelnost (maintainability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) být modifikovatelný. Udržovatelnost zahrnuje tyto atributy:
  - Analyzovatelnost (analysability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) ulehčit nalezení vady v případě výskytu poruchy a schopnost určit, co se má změnit, aby byla vada odstraněna.
  - Měnitelnost (changeability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) ulehčit uskutečňování modifikací.
  - Stabilita (stability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) zabránit nežádoucím důsledkům uskutečněných modifikací.
  - Testovatelnost (testability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) zabezpečit lehkou validaci po provedení modifikací.
- Přenositelnost (portability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) být přenesený z jednoho prostředí do jiného. Přenositelnost informačního systému (softwarového produktu) zahrnuje tyto atributy:
  - Přizpůsobitelnost (adaptability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) být přizpůsobitelný různým prostředím, ve kterých má být využíván, a to vlastními prostředky, které jsou jeho součástí.
  - Instalovatelnost (installability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) být zavedený tak, aby vyhovoval použití a práci v konkrétním prostředí.
  - Slučitelnost (co-existence). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) pracovat společně s jinými

informačními systémy (softwarovými produkty) ve společném prostředí a využívat společné zdroje.

- Nahraditelnost (replaceability). Tento atribut je vymezen jako schopnost informačního systému (softwarového produktu) nahradit funkci jiných systém, určených pro stejný účel a pracujících ve stejném, nebo podobném prostředí.

Některé požadavky nelze jednoznačně zařadit ani do jedné kategorie. Proto v každé z uvedených šesti charakteristik jsou vyčleněny další podcharakteristiky. Ani tyto podcharakteristiky nelze však stále měřit, měřitelnými vlastnostmi jsou až jejich atributy. Každá podcharakteristika může být charakterizována více atributy:

- Vnější atributy – lze je získat pozorováním funkce produktu při jeho používání.
- Vnitřní atributy – analyzuje se samotný produkt.

Vnější atributy jsou ukazateli jakosti, zatímco vnitřní jsou spíše prediktory jakosti, avšak na jejich základě lze usuzovat, jakou úroveň jakosti bude daný produkt mít. Jejich výhodou je možnost měření dříve, než je produkt dokončen, někdy i v samotných počátcích cyklu produktu. To je samozřejmě obrovskou výhodou, neboť v této fázi je ještě náprava relativně snadná a méně nákladná.

K měření kvality a jakosti informačních systémů se používají metriky. Pavel Učeň v knize Metriky v informatice [1] definuje metriku jako přesně vymezený finanční či nefinanční ukazatel nebo hodnotící kritérium, které jsou používány k hodnocení úrovně efektivnosti konkrétní oblasti řízení podnikového výkonu a jeho efektivní podpory prostředky IS/IT. Skupinu metrik sdružených za určitým cílem pak nazývá portfoliem metrik. Softwarové metriky umožňují organizacím měřit, řídit a odhadovat softwarové projekty, ale v současnosti se soustředí převážně na měření údajů týkajících se složitosti nebo kvality softwaru.
Existuje velké množství již navržených metrik pro hodnocení úrovně bezpečnosti informací. Metrika by měla vyhovovat několika základním požadavkům:

- měření bylo objektivní,
- získání vstupních dat by nemělo být nákladné měření mohlo být prováděno opakovaně,
- výsledek měření mohl být vyjádřen jako číslo či procento výsledek měření byl vztažen ke konkrétní veličině.

Existuje mnoho způsobů, jak kategorizovat metriky. Různí autoři používají odlišná dělení.

Z obecného hlediska lze metriky rozdělit na tvrdé a měkké. Dále pak například z pohledu úrovně řízení na metriky operativní, taktické a strategické. Lze také metriky rozčlenit dle opakovatelnosti použití na metriky kontinuální a diskrétní či z pohledu hodnocení efektivnosti inovace IS/IT na metriky interní a externí.

- *Tvrdé a měkké metriky.* Tvrdá metrika je objektivně měřitelný ukazatel, který by měl být lehce měřitelný a levný. To znamená k dispozici bez dodatečných nákladů. Výsledkem tvrdé metriky by měla být konkrétní hodnota, ve většině případů převeditelná na finanční vyjádření. Mimo ukazatelů existují také indikátory, což jsou metriky, které mají stanoveny meze, které představují žádoucí stav. Jakákoli

odchylka od ideální hodnoty směrem k horšímu znamená problém (nežádoucí stav). Měkké metriky jsou naopak takové ukazatele, které nejsou objektivně měřitelné. Jedná se o subjektivní vyjádření určitého stavu, kupříkladu úrovně spokojenosti zákazníka či pověsti podniku (zlepšení jeho dobrého jména).

- *Kontinuální a diskrétní metriky*. Pokud měření probíhá opakovaně v předem stanovené periodě, jedná se o metriky kontinuální. Oproti tomu diskrétní metriky jsou aplikovány sice opakovaně, ale pouze v časově omezeném období. Kupříkladu během inovace zařízení, kdy srovnáváme aktuální stav se stavem před inovací.

- *Metriky z pohledu úrovní řízení*. Z pohledu úrovní řízení lze metriky rozdělit na operativní, strategické a taktické. Strategické metriky představují především kontinuální tvrdé metriky (v nejlepším případě indikátory). Výsledky těchto metrik jsou určeny především pro vedení organizace. Operativní metriky pak mohou být jak tvrdé, tak i měkké metriky, které by měly poskytovat informace o provozu. Metriky taktické úrovně pak představují zejména výsledkové metriky. To jest takové ukazatele, které jsou zaměřeny na dosahování cílů (porovnání skutečného stavu oproti našim plánům).

- *Interní, externí metriky*. Z pohledu hodnocení efektivnosti inovace IS/IT lze metriky rozčlenit na metriky interní a externí. Interní metriky jsou určeny především k hodnocení efektivnosti vložených prostředků a úrovně poskytovaných služeb. Tyto metriky navrhuje přímo uživatelský podnik. Externí metriky pak jsou navrhovány nejen uživatelským podnikem, ale i subjektem, který se podílí na inovaci IS/IT. Externí metriky lze tedy jinak označit jako metriky dodavatelské.

Bezpečnost informačních systémů se zaměřuje na tři komponenty, a to

- *Dostupnost data a služeb*
- *Důvěrnost.* K aktivům (data, SW, HW) mají přístup pouze autorizované subjekty. Lze jí zabezpečit pomocí šifrování, skrýváním identit počítačů organizace za firewally nebo řízením přístupu k souborům.
- *Integrita dat***.** Vlastnost, která zaručuje, že na stejnou otázku dostanu od IS vždy stejnou odpověď. Jedné se o celistvost dat a služeb.

Problematika kvality a jakosti informačních systémů poskytuje komplexní pohled na informační systém a umožňuje identifikovat komponenty informačního systému, na které lze aplikovat bezpečnostní testy (hledisko dostupnosti, důvěrnosti a integrity dat). Metriky jsou vhodným prostředkem ke kvantifikaci zjišťovaných atributů nejen kvality a jakosti, ale i bezpečnosti informačních systémů.

Literatura

[1] UČEŇ, Pavel, et al. *Metriky v informatice : Jak objektivně zjistit přínosy informačního systému*. První vydání Praha : Grada Publishing, 2001. 139 s. ISBN 80-247-0080-8.

[2] http://si.vse.cz/archive/proceedings/2001/metriky-jako-nastroj-rizeni-efektivity-is-it.pdf

[3] [1] Vaníček, J.: Měření a hodnocení jakosti informačních systémů, druhé rozšířené vydání, Česká

[4] zemědělská univerzita v Praze, PEF, 2004, 328 stran, ISBN 80-213-1206-6

[5] [2] Vaníček, J.: Software and Data Quality, Agriculture Economics, 52, 2006 (3), pp. 138 – 146

[6] [3] Vaníček, J.: Software quality measures validation in Czech Republic, Agriculture Economics, 53,

[7] 2007(3), p. 94 - 100

[8] [4] Vaníček, J.: Software quality requirements, Agriculture Economics, 52, 2006 (4), p. 177 - 18

Tento příspěvek byl zpracován v rámci Projektu vědeckovýzkumného úkolu č. 4/4 „Informační bezpečnost a kybernetická kriminalita v organizaci“, který je součástí Integrovaného výzkumného úkolu na léta 2010-2015, realizovaný Fakultou bezpečnostního managementu Policejní akademie České republiky v Praze.