

Y36BEZ – Bezpečnost přenosu a zpracování dat

Róbert Lórencz

10. přednáška

Informační bezpečnost 1

<http://service.felk.cvut.cz/courses/Y36BEZ>
lorencz@fel.cvut.cz

- Komponenty informační bezpečnosti
- Základní pojmy a definice
- Architektura informační bezpečnosti v modelu OSI

Komponenty informační bezpečnosti (1)

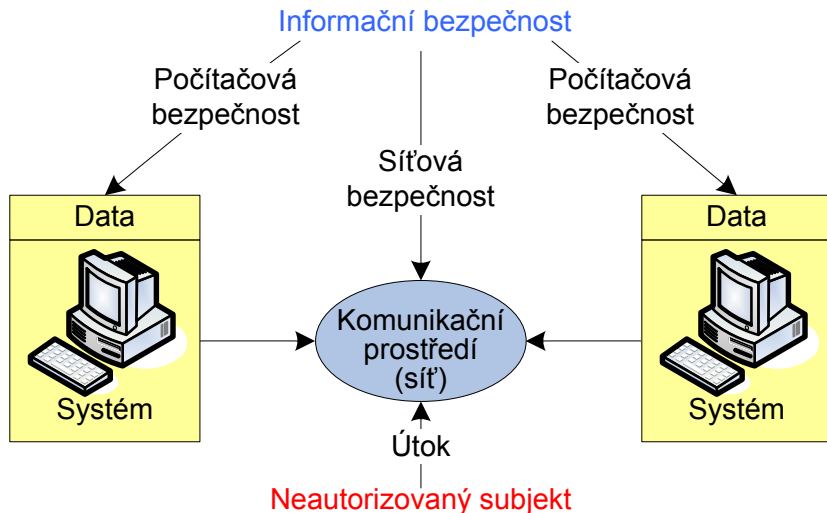
- 1 **Informační technologie – IT** → technologie na zpracování informací.
- 2 **Informační a komunikační technologie – ICT** → technologie zahrnující jak počítačové systémy tak také telekomunikační sítě pro zpracování informací.

ICT – soubor technických, programových a komunikačních prostředků pro zpracování a přenos informací s využitím počítačů, komunikujících přes komunikační prostředí. Systémy na bázi IT, resp. ICT se označují jako **IT systémy**, resp. **ICT systémy**.

- Zpracování a přenos informací vyžadují řešit otázky bezpečnosti IT a ICT systémů.
- Bezpečnost těchto systémů řeší **informační bezpečnost**, která se skládá z:
 - 1 počítačové bezpečnosti (computer security),
 - 2 síťové bezpečnosti (network security).

Komponenty informační bezpečnosti (2)

Komponenty informační bezpečnosti



Komponenty informační bezpečnosti (3)

Počítačová bezpečnost představuje souhrn prostředků zabezpečujících bezpečný provoz počítačů a ochranu dat zpracovaných a uchovaných počítači.

Síťová bezpečnost představuje souhrn prostředků zabezpečujících ochranu dat po dobu jejich přenosu komunikačním prostředím a ochranu počítačů připojených do počítačové sítě.

- Hranice mezi počítačovou a sítíovou bezpečností jsou neostré.
- Například viry, které představují nejznámější způsob útoku na informační systémy, mohou narušit počítačovou bezpečnost přes zavírovaná média nebo také přes počítačovou síť.

Pro vysvětlení principů, kterými se zabývá **informační bezpečnost**, se vyžaduje vymezit a definovat některé základní pojmy a definice vycházející z platných norem pro oblast IT a ICT.

Základní pojmy a definice (1)

Definice Informační bezpečnosti

Souhrn prostředků a postupů na zabezpečení důvěrnosti, integrity a dostupnosti informací, na zabezpečení autentizace uživatelů a zdrojů, účtovatelnosti operací, jakož i zabezpečení ochrany proti neautorizované manipulaci, modifikaci nebo zničení, resp. poškození informací v informačním systému.

Důvěrnost (confidentiality) je vlastnost, která zaručuje, že informace nebude dostupná neautorizovanému subjektu.

Integrita (integrity) je vlastnost, která zaručuje úplnost a přesnost zpracované, resp. přenášené informace.

Dostupnost (availability) je vlastnost, která zaručuje, že informace bude dostupná autorizovanému subjektu.

Informační bezpečnost se vždy vztahuje na určitý celek, který se označuje jako **informační systém** (IS) (information system).

Základní pojmy a definice (2)

IS je funkční celek, který systematicky a cílevědomě zabezpečuje získávání, shromažďování, zpracování, uchovávání a poskytování informací podle dopředu definovaných postupů.

Vše, co představuje určitou hodnotu pro organizaci, firmu nebo jiný ekonomický subjekt, označujeme jako **užitkovou hodnotu** (asset).

Struktura IS zahrnuje užitkové hodnoty, které lze rozdělit do kategorií:

- **Hmotné užitkové hodnoty** (physical assets): hlavně technické prostředky (počítačový a komunikační HW, budovy atd.).
- **Nehmotné užitkové hodnoty** (nonphysical assets): SW, informace (data), resp. schopnost poskytovat informace a služby.
- **Lidské zdroje** (human resources): personál provozující IS.

Užitkové hodnoty jsou vystavené různým typům **ohrožení** (threats) představujících potenciálně narušení bezpečnosti IS a následné ztráty resp. škody v IS.

Základní pojmy a definice (3)

- Ohrožení mohou být:
 - ▶ **Úmyslná**: odposlech, modifikace informace, neautorizovaný přístup do IS atd. Subjekt generující umyslné ohrožení – **útok** (attack) je **útočník** (intruder).
 - ▶ **Neumyslná**: chyby způsobené nesprávnou obsluhou IS (neumyslné mazání souborů, nekorektní využívání HW a SW IS).
- Ohrožení mohou mít původ v přírodním prostředí (živ. pohromy).
- Charakteristiky ohrožení definující vztah k jiným mechanismům bezpečnosti jsou:
 - ▶ zdroj ohrožení,
 - ▶ motivace ohrožení,
 - ▶ početnost výskytu ohrožení,
 - ▶ pravděpodobnost výskytu ohrožení,
 - ▶ dopad ohrožení.
- Z hlediska **přístupu** do IS můžeme ohrožení rozdělit na:
 - 1 softwarové,
 - 2 ohrožení neautorizovaným subjektem.

Základní pojmy a definice (4)

- **Softwarové ohrožení** je způsobené **viry** a **červy**. Pronikají do interního prostředí poč. systémů při legální výměně zpráv mezi těmito systémy přes poč. síť nebo přes paměťová média zavedená do těchto systémů.
- **Ohrožení neautorizovaným subjektem** – útočníkem – je potencialní ohrožení získáním přístupu do IS s rizikem způsobení ztrát nebo škod v tomto IS.

Pokud útok ovlivní více užitkových hodnot IS, může to vyvolat různé dopady na IS v závislosti na napadené složce.

Ohrožení lze klasifikovat třemi stupni: **nízké, střední a velké ohrožení**

Zranitelnost (vulnerability) je slabé místo IS, které může být využité ohrožením na způsobení ztráty nebo škody v IS.

Základní pojmy a definice (5)

- Zranitelnost nezpůsobuje škody nebo ztráty v IS, vytváří ale pro to podmínky.
- Zranitelnost – slabá místa – mohou být vytvořena na všech úrovních, složkách IS: fyzická vrstva, HW, SW, organizační, personální struktura, management a administrace IS.
- Například zranitelná může být slabá úroveň řízení a kontroly přístupu, nedostatečná antivirová ochrana atd.
- Známe 3 úrovně zranitelnosti **nízká, střední a vysoká**.

Incident informační bezpečnosti (information security incident) je jakákoliv neočekávaná a nežádoucí událost způsobující selhání nebo nesprávnou činnost IS.

Například incident informační bezpečnosti může být odmítnutí služby IS, nezvládnutelné změny v IS atd.

Základní pojmy a definice (6)

Výsledek incidentu informační bezpečnosti vyvolaný ohrožením a ovlivňující činnost IS se nazývá **dopad** (impact).

- Dopad se může projevit destrukcí některé složky IS, ztrátou nebo škodou v IS.
- Může dojít k narušení důvěrnosti a integrity dat nebo ztrátou dostupnosti dat v IS ⇒ **přímý dopad** na IS (direct impact).
- **Nepřímý dopad** (indirect impact) zahrnuje finanční ztráty, ztrátu konkurenční schopnosti a postavení na trhu organizace, která IS používá.

Posouzení dopadu (assessment of impact) je založen na porovnání předpokládaných výsledků incidentů informační bezpečnosti a cenou prostředků na zabezpečení dostatečné úrovně bezpečnosti, která by eliminovala výskyt incidentů informační bezpečnosti.

Základní pojmy a definice (7)

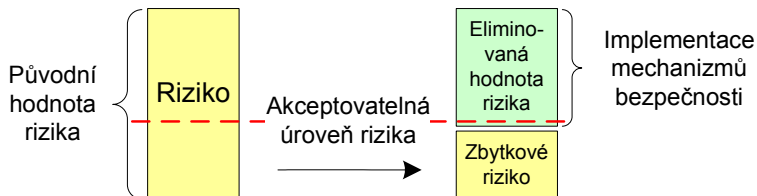
Definice rizika

Riziko představuje potencialní možnost vzniku určité ztráty nebo škody v IS tím, že ohrožení využije zranitelnost složek IS.

- Riziko je charakterizované kombinací dvou faktorů:
pravděpodobnosti vzniku incidentu informační bezpečnosti a dopadem.
- Jakákoliv změna v užitkových hodnotách IS a mechanismech bezpečnosti může významně ovlivnit riziko.
- Riziko nemůžeme nikdy úplně eliminovat.
- Aplikací mechanismů bezpečnosti lze snížit hodnoty rizika na akceptovatelnou úroveň.
- Zůstatková hodnota rizika se označuje jako reziduální – zbytkové riziko (residual risk).

Základní pojmy a definice (8)

Vliv implementace mechanismů bezpečnosti na riziko



Analýza rizika (risk analysis): systematický proces odhadu velikosti rizika.

Posouzení rizika (risk assessment): proces identifikace a analýzy rizika.

Management rizika (risk management): proces identifikace, řízení, eliminace a minimalizace rizika.

Základní pojmy a definice (9)

Mechanismy bezpečnosti (security mechanism, safeguards): postupy nebo procedury, které realizují ochranu proti ohrožení, snižují úroveň zranitelnosti a omezují dopad incidentů informační bezpečnosti.


- Na zvýšení úrovně informační bezpečnosti se využívá více mechanismů.
- Mechanismy bezpečnosti mohou realizovat jednu nebo více funkcí: prevence, detekce útoků, omezení ohrožení, obnova funkce atd.

Omezení (constraints): omezující faktory, které určují a limitují činnost IS v podmínkách jeho existence.

- Příklady omezení jsou: organizační, obchodní, personální, enviromentální, technické, socialní, atd.

Základní pojmy a definice (10)

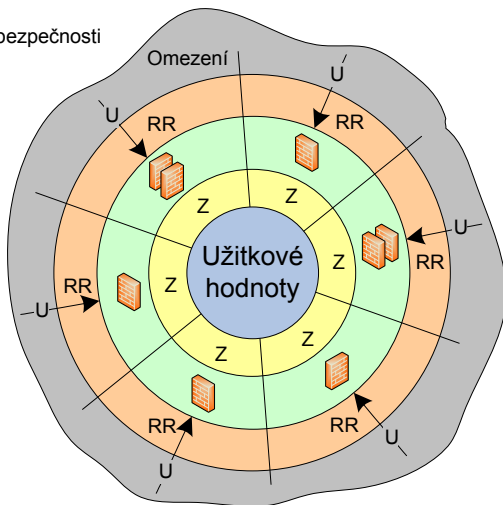
Vztah mezi složkami informační bezpečnosti

 - Mechanismus bezpečnosti

RR - Zbytkové riziko

U - Útočník

Z - Zranitelnost



Architektura informační bezpečnosti v modelu OSI (1)

Systematický přístup k bezpečnosti otevřených systémů představuje doporučení ITU-T s označením X.800 vázané na model OSI (Open System Interconnection). Architektura v OSI byla přijata jako mezinárodní standard a zahrnuje:

- **Služby bezpečnosti** (security services): definované postupy zvyšující bezpečnost IS a realizující ochranu proti útokům na tyto systémy. Služby bezpečnosti využívají jeden nebo několik mechanismů.
- **Mechanismy bezpečnosti** (security mechanisms, safeguards): definované postupy na detekci a prevenci proti útokům na bezpečnost nebo definované postupy na odstranění následků těchto útoků na bezpečnost.
- **Útoky na bezpečnost** (security attacks): jakákoliv cílevědomá (úmyslná) činnost snižující nebo narušující bezpečnost. Z tohoto pohledu lze útok popsat jako úmyslné ohrožení generované entitou uměle, cílevědomě a inteligentně (intelligent threat).

Architektura informační bezpečnosti v modelu OSI (2)

Služby bezpečnosti

Doporučení X.800 definuje službu bezpečnosti jako službu realizovanou příslušným protokolem vrstvy ISO, který zajišťuje adekvátní bezpečnost otevřeného systému nebo přenosu dat.

Služby bezpečnosti jsou v doporučení ISO rozdělené do pěti kategorií:

- autentizace (authentication),
- řízení přístupu (access control),
- zabezpečení důvěrnosti dat (data confidentiality),
- zabezpečení integrity dat (data integrity),
- ochrana proti odmítnutí původu zpravy (nonrepudiation).

Autentizace je služba bezpečnosti, úlohou které je zaručit nebo ověřit, že komunikace je autentická.

V doporučení X.800 jsou definované dvě specifické služby autentizace:

Architektura informační bezpečnosti v modelu OSI (3)

- Autentizace komunikujících uživatelů (peer entity authentication): zabezpečuje potvrzení identity uživatelů v průběhu přenosu.
- Autentizace zdroje dat (data origin authentication): zabezpečuje identity zdroje dat, ale nezabezpečuje ochranu před duplicitou nebo modifikací datových jednotek. Tento typ služby podporuje aplikace jako je např. elektronická pošta.

Řízení přístupu je služba bezpečnosti, která na základě autentizace uživatele a jemu přidělených práv umožňuje jeho přístup do systému nebo k systémovým prostředkům a službám přes komunikační kanály.

- Rozsah přístupu je určen přidělenými právy ⇒
- zákaz přístupu do systému neautorizovaným subjektům.

Zabezpečení důvěrnosti dat je služba bezpečnosti, která zabezpečuje ochranu informačního obsahu dat, tj. ochranu dat před jejich odhalením neautorizovaným subjektem.

Architektura informační bezpečnosti v modelu OSI (4)

- Důvěrnost dat je potřeba zabezpečit v režimu přenosu dat při *spojově orientované komunikaci* (connection confidentiality) nebo při *komunikaci bez spojové orientace* (connectionless confidentiality).
- Zabezpečení důvěrnosti se může vztahovat na celý blok dat nebo specifikovanou část bloku dat (selective-field confidentiality).
- Další aspekt důvěrnosti dat je ochrana toku dat vůči jeho analýze nepovolaným subjektem (traffic-flow confidentiality).
 - ▶ Nepovolaný subjekt nemůže potom identifikovat zdroj nebo adresáta dat při jejich přenosu
 - ▶ Nemůže taky identifikovat systémové parametry toku dat (délka, rychlost přenosu, atd.).

Architektura informační bezpečnosti v modelu OSI (5)

Zabezpečení integrity dat je služba bezpečnosti zabezpečující kontrolu integrity dat, tj. zdali nedošlo k jejich neautorizované modifikaci.

- Integritu možno aplikovat na celý tok dat, na jednotlivé bloky dat nebo na vybrané pole v bloku dat.
- Ve spojově orientovaných službách se integrita vztahuje na celý tok dat.
- Zabezpečení integrity umožňuje zjistit, zdali přijatá zpráva je totožná s vyslanou zprávou a zdali nebyla modifikována, duplikována, doplněna nebo přeuspořádána po dobu přenosu. Současně je zabezpečena identifikace poškození zprávy.
- Ve službách bez spojové orientace se integrita vztahuje jen na individuální bloky dat.
- Služby zabezpečující integritu lze rozdělit na služby zabezpečující *integritu s obnovením* a *bez obnovení* integrity dat (services with/without recovery).

Architektura informační bezpečnosti v modelu OSI (6)

Ochrana proti odmítnutí původu dat je služba bezpečnosti zabezpečující důkaz o původu vyslaných dat specifikovaným subjektem resp. o přijetí dat specifikovaným subjektem.

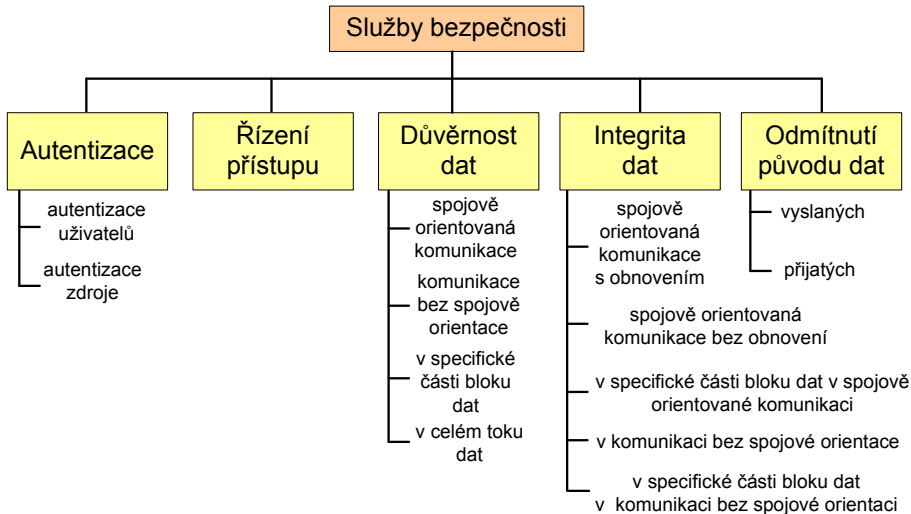
- Lze rozlišit službu zabezpečující ochranu proti odmítnutí vyslaných dat (nonrepudiation-origin) a
- službu zabezpečující ochranu proti odmítnutí přijatých dat (nonrepudiation-destination).
- Zabraňuje popření odpovědnosti za vyslaná nebo přijatá data.

Služba dostupnosti (availability service): služba, která zajišťuje dostupnost systému a poskytuje ochranu proti útokům na dostupnost.

- X.800 definuje dostupnost: vlastnost systému zabezpečit dostupnost informací autorizovanému subjektu v souladu se specifikací systému a jeho návrhem.
- Různé útoky jsou zaměřeny právě na ztrátu nebo redukci dostupnosti ⇒ odmítnutí služby (denial of service).

Architektura informační bezpečnosti v modelu OSI (7)

Přehled služeb bezpečnosti



Architektura informační bezpečnosti v modelu OSI (8)

Mechanismy bezpečnosti: podporují služby bezpečnosti a realizují specifické činnosti zaměřené na ochranu proti útokům resp. jejich následkům. Lze je rozdělit na mechanismy bezpečnosti *implementované ve specifikované protokolové vrstvě* a *implementované v libovolné protokolové vrstvě*. Mezi základní mechanismy bezpečnosti patří:

- šifrování (encipherment),
- digitální podpisy (digital signature),
- řízení přístupu (access control),
- integrita dat (data integrity),
- výměna autentizační informace (authentication exchange),
- vyplňování mezer (traffic padding),
- řízení směrování (routing control),
- osvědčení třetím subjektem (notarization).

Architektura informační bezpečnosti v modelu OSI (9)

Šifrování: mechanismus bezpečnosti zabezpečující utajení informačního obsahu zprávy s využitím určité kryptografické transformace na úpravu zprávy do formy, která je nečitelná neautorizovaným subjektem.

Digitální podpisy: mechanismy bezpečnosti využívající kryptografických transformací na zabezpečení autentizace zdroje zprávy a integrity dat.

Řízení přístupu: zahrnuje širokou třídu mechanismů bezpečnosti zabezpečující řízení a kontrolu přístupových práv k systémovým prostředkům a službám.

Integrita dat: zahrnuje mechanismy kontroly integrity přenášených dat.

Výměna autentizační informace: proces výměny autentizační informace mezi uživatelem a IS. Slouží pro ověření identity uživatele a její výsledek ovlivňuje řízení přístupu k systémovým prostředkům a službám IS.

Architektura infor. bezpečnosti v modelu OSI (10)

Vyplňování mezer: mechanismus bezpečnosti realizující vkládání dodatečných bitů do mezer mezi daty s cílem znemožnit analýzu toku dat.

Řízení směrování: mechanismus bezpečnosti umožňující selekci fyzických přenosových cest pro určitá data a dovoluje změnu směrování a to hlavně v případech, kdy se očekává narušení bezpečnosti.

Osvědčení třetím (důvěryhodným) subjektem: mechanismus bezpečnosti využívající třetí subjekt na zabezpečení určitých bezpečnostních aspektů v IS.

Následující tabulka ilustruje vztah mezi službami bezpečnosti a mechanismy bezpečnosti podle X.800.

Architektura infor. bezpečnosti v modelu OSI (11)

Služby a mechanismy bezpečnosti

	Šifrování	Digitální propisy	Řízení přístupu	Integrita dat	Autentizační výměna	Vyplňování mezer	Řízení směrování	Osvědčení 3. subjektem
Autentizace uživatelů	Ano	Ano			Ano			
Autentizace zdroje dat	Ano	Ano						
Řízení přístupu			Ano					
Zabezpečení důvěryhodnosti dat	Ano						Ano	
Ochrana toku dat	Ano					Ano	Ano	
Zabezpečení integrity dat	Ano	Ano		Ano				
Odmítnutí služby		Ano		Ano				Ano
Dostupnost			Ano	Ano				

Útoky na bezpečnost

Útoky na bezpečnost můžeme podle X.800 rozdělit do dvou kategorií:

- **Pasivní útoky** (passive attacks): útoky na bezpečnost zaměřené na získání informací z IS, resp. na jejich využití. Neovlivňují systémové prostředky IS.
- **Aktivní útoky** (active attacks): útoky na bezpečnost. Kromě získání informací a modifikací toku dat se pokoušejí ovlivnit také systémové prostředky a jejich činnost.

Pasivní útoky na bezpečnost

Využívají hlavně sledování (odposlech) nebo monitorování provozu s využitím dvou základních přístupů:

- **Odkrývání obsahu zpráv** (release of message content): využívá sledování a monitorování. Účinné jenom v případě, když komunikace probíhá v otevřené formě.

- **Analýza toku dat** (traffic analysis): je zaměřená na získávání informací ze zachyceného toku dat jeho analýzou. Ochrana proti těmto útokům se zakládá na předpokladu, že jsou těžce detekovatelné, protože neovlivňují tok dat a systémové prostředky. Základním mechanismem na ochranu přenášené zprávy je šifrování.

Aktivní útoky na bezpečnost

Modifikují přenášený tok dat nebo vytvářejí falešný tok dat. Můžeme je rozdělit do 4 kategorií:

- předstírání identity (masquerade),
- opakování (replay),
- modifikace zpráv (modification of messages),
- odmítnutí služby (denial of service).

Architektura inf. bezpečnosti v modelu OSI (14)

Předstírání identity: útočník předstírá identitu jiného subjektu. Výměna autentizační informace s autorizovaným subjektem je zachycená útočníkem - neautorizovaným subjektem. Umožňuje útočníkovi získat práva přidělená autorizovanému subjektu.

Útok opakováním: jsou zachycená data a jejich subsekvence se vyšle s opožděním do IS za účelem vyvolání nežádoucích (neautorizovaných) efektů.

Modifikace zprávy: určitá část původní přenášené zprávy je útokem změněná nebo je zpráva opožděná nebo přeuspořádaná, což vyvolá nežádoucí (neautorizované) efekty.

Odmítnutí služby: aktivní útok zabráňující standardnímu využití služby nebo managementu sítě. Útok může mít specifický cíl, případně neautorizovaný subjekt může potlačit všechny zprávy směřující k jinému subjektu.

Architektura inf. bezpečnosti v modelu OSI (15)

Další forma odmítnutí služby je rozpad sítě, zamezení přístupu do sítě nebo zahlcení sítě zprávami s cílem degradace její výkonnosti. Dokonalejší varianta je útok vedený více počítači na jeden server - distribuovaný útok DDos (Distributed Denial of Service).

- Pasivní útoky lze těžko detekovat.
- Aktivní útoky se projeví okamžitě nebo s malým zpožděním - jejich účinky jsou evidentní.
- Úplná ochrana proti aktivním útokům je obtížná, vyžaduje neustálou fyzickou ochranu všech komunikačních prostředků a kanálů.
- Cílem ochrany je detekce útoků a odstranění jejich následků.
- Lze kalkulovat i s odstrašujícím faktorem.