VYHLÁŠKA 523-2005

Vymezení pojmů:

a) aktivem informačního systému na základě analýzy rizik (§ 11) definovaný hardware, software, dokumentace informačního
systému a utajované informace, které jsou v informačním systému uloženy,
b) objektem informačního systému pasivní prvek informačního systému, který obsahuje nebo přijímá informaci,
c) subjektem informačního systému aktivní prvek informačního systému, který způsobuje předání informace mezi objekty
informačního systému nebo změnu stavu systému,
d) analýzou rizik proces, během něhož jsou zjišťována aktiva informačního systému, hrozby působící na aktiva informačního
systému, jeho zranitelná místa, pravděpodobnost realizace hrozeb a odhad jejich následků,
e) auditním záznamem záznam informačního systému o události, která může ovlivnit bezpečnost informačního systému,
f) identifikací subjektu informačního systému proces zjištění jeho identity v informačním systému,
g) autentizací subjektu informačního systému proces ověření jeho identity v informačním systému, splňující požadovanou míru
záruky,
h) autorizací subjektu informačního systému udělení určitých práv pro vykonávání určených aktivit v informačním systému,
i) důvěrností utajované informace její vlastnost, která znemožňuje odhalení utajované informace neoprávněné osobě,
j) fyzickou bezpečností informačního systému nebo komunikačního systému opatření použitá k zajištění fyzické ochrany aktiv
těchto systémů proti náhodným nebo úmyslným hrozbám,
k) integritou aktiva informačního systému nebo komunikačního systému vlastnost, která umožňuje provedení jeho změny určeným
způsobem a pouze oprávněným subjektem informačního systému,
l) komunikační bezpečností opatření použitá k zajištění ochrany utajovaných informací při přenosu definovaným komunikačním
prostředím,
m) počítačovou bezpečností bezpečnost informačního systému zajišťovaná jeho technickými a programovými prostředky,
n) povinným řízením přístupu prostředky pro omezení přístupu subjektů informačního systému k objektům informačního systému,
založené na porovnání stupně utajení utajované informace obsažené v objektu informačního systému a úrovně oprávnění subjektu informačního systému pro přístup k utajované informaci a zajišťující správný tok informací mezi objekty informačního
systému s různými stupni utajení, nezávisle na volbě učiněné uživatelem,
o) rizikem pro informační systém nebo komunikační systém pravděpodobnost, že určitá hrozba využije zranitelných míst

některého z těchto systémů,
p) rolí souhrn určených činností a potřebných autorizací pro subjekt informačního systému působící v informačním systému nebo
komunikačním systému,
q) bezpečnostním správcem informačního systému nebo komunikačního systému pracovník správy informačního systému nebo
komunikačního systému v roli vytvořené pro řízení a kontrolu bezpečnosti informačního systému nebo komunikačního systému a
provádění stanovených činností pro zajištění bezpečnosti informačního systému nebo komunikačního systému,
r) správcem informačního systému nebo komunikačního systému pracovník správy informačního systému nebo komunikačního
systému v roli vytvořené zejména pro zajištění požadované funkčnosti informačního systému nebo komunikačního systému a
řízení provozu informačního systému nebo komunikačního systému,
s) uživatelem informačního systému nebo komunikačního systému fyzická osoba v roli vytvořené zejména pro nakládání s
utajovanými informacemi v informačním systému nebo pro přenos utajovaných informací v komunikačním systému,
t) řízením přístupu prostředky pro omezení přístupu subjektů informačního systému k objektům informačního systému, zajišťující,
že přístup k nim získá jen autorizovaný subjekt informačního systému,
u) volitelným řízením přístupu prostředky omezení přístupu subjektů informačního systému k objektům informačního systému,
založené na kontrole přístupových práv subjektu informačního systému k objektu informačního systému, přičemž uživatel, správce
nebo bezpečnostní správce informačního systému vybavený určitými přístupovými právy pro přístup k objektu informačního
systému může zvolit, na které další subjekty informačního systému přenese přístupová práva k tomuto objektu informačního
systému, a může tak ovlivňovat tok informace mezi objekty informačního systému,
v) bezpečnostním standardem utajovaný soubor pravidel, ve kterém se stanoví postupy, technická řešení, bezpečnostní
parametry a organizační opatření pro zajištění nejmenší možné míry ochrany utajovaných informací,
w) bezpečnostním provozním módem prostředí, ve kterém informační systém pracuje, charakterizované stupněm utajení
zpracovávané utajované informace a úrovněmi oprávnění uživatelů,
y) nepopiratelností schopnost prokázat zpětně jednání či událost tak, aby dané jednání či událost nemohly být následně popřeny,

Bezpečnost informačních systémů

(1) Bezpečnosti informačního systému se dosahuje uplatněním souboru opatření z oblasti
a) počítačové a komunikační bezpečnosti,
b) kryptografické ochrany,
c) ochrany proti úniku kompromitujícího vyzařování,
d) administrativní bezpečnosti a organizačních opatření,
e) personální bezpečnosti a
f) fyzické bezpečnosti informačního systému.

Bezpečnostní dokumentace informačního systému

(1) Bezpečnostní dokumentaci informačního systému tvoří
a) projektová bezpečnostní dokumentace informačního systému a
b) provozní bezpečnostní dokumentace informačního systému.
(2) Projektová bezpečnostní dokumentace informačního systému obsahuje
a) bezpečnostní politiku informačního systému a výsledky analýzy rizik,
b) návrh bezpečnosti informačního systému zajišťující splnění bezpečnostní politiky informačního systému, přičemž podrobnost
jeho popisu musí umožnit přímou realizaci navrhovaných opatření, a
c) dokumentaci k testům bezpečnosti informačního systému.
(3) Provozní bezpečnostní dokumentace informačního systému obsahuje
a) bezpečnostní směrnice informačního systému, které předepisují činnost bezpečnostních správců informačního systému v
jednotlivých rolích zavedených v informačním systému pro zajištění bezpečnostní správy informačního systému,
b) bezpečnostní směrnice informačního systému, které předepisují činnost správců informačního systému v jednotlivých rolích
zavedených v informačním systému pro správu informačního systému, pokud se týká zajištění bezpečnosti informačního systému, a
c) bezpečnostní směrnice informačního systému, které předepisují činnost uživatelů informačního systému, pokud se týká
zajištění bezpečnosti informačního systému.

Bezpečnostní politika informačního systému

(1) Pro každý informační systém musí být již v počáteční fázi jeho vývoje zpracována bezpečnostní politika informačního
systému.

Požadavky na formulaci bezpečnostní politiky informačního systému

Bezpečnostní politika informačního systému se formuluje na základě

a) minimálních bezpečnostních požadavků v oblasti počítačové bezpečnosti,
b) systémově závislých bezpečnostních požadavků, požadavků uživatele a výsledků analýzy rizik a
c) bezpečnostních požadavků bezpečnostní politiky nadřízeného orgánu, pokud byla zpracována.

Minimální bezpečnostní požadavky v oblasti počítačové bezpečnosti

(1) Informační systém nakládající s utajovanými informacemi stupně utajení Důvěrné nebo vyššího musí zajišťovat tyto
bezpečnostní funkce

a) jednoznačnou identifikaci a autentizaci uživatele, bezpečnostního správce nebo správce informačního systému, které musí
předcházet všem jejich dalším aktivitám v informačním systému a musí zajistit ochranu důvěrnosti a integrity autentizační
informace,
b) volitelné řízení přístupu k objektům informačního systému na základě rozlišování a správy přístupových práv uživatele,
bezpečnostního správce nebo správce informačního systému a jejich identity nebo jejich členství ve skupině uživatelů,
bezpečnostních správců nebo správců informačního systému,
c) nepřetržité zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením. Zaznamenává se zejména
použití identifikačních a autentizačních informací, pokusy o zkoumání přístupových práv, vytváření nebo rušení objektu
informačního systému nebo činnost autorizovaných subjektů informačního systému ovlivňující bezpečnost informačního systému,
d) možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého uživatele, bezpečnostního správce nebo správce
informačního systému,
e) ošetření paměťových objektů před jejich dalším použitím, zejména před přidělením jinému subjektu informačního systému,
které znemožní zjistit jejich předchozí obsah, a
f) ochranu důvěrnosti dat během přenosu mezi zdrojem a cílem.

Systémově závislé bezpečnostní požadavky odvozené z bezpečnostního provozního módu

(1) Informační systémy se mohou provozovat pouze v některém z uvedených bezpečnostních provozních módů, jimiž
jsou:

a) bezpečnostní provozní mód vyhrazený,
b) bezpečnostní provozní mód s nejvyšší úrovní,
c) bezpečnostní provozní mód s nejvyšší úrovní s formálním řízením přístupu k informacím, nebo
d) bezpečnostní provozní mód víceúrovňový.

(2) Bezpečnostní provozní mód vyhrazený je takové prostředí, které umožňuje zpracování utajovaných informací
různého stupně utajení, přičemž všichni uživatelé musí splňovat podmínky pro přístup k utajovaným informacím nejvyššího stupně
utajení, které jsou v informačním systému obsaženy, a zároveň musí být oprávněni pracovat se všemi utajovanými informacemi,
které jsou v informačním systému obsaženy. Bezpečnost informačního systému, který je provozován v bezpečnostním provozním
módu vyhrazeném, se zabezpečuje splněním minimálních bezpečnostních požadavků v oblasti počítačové bezpečnosti
uvedených v § 7 odst. 1 písm. a), c), d) a f) a dále opatřeními z oblasti administrativní a personální bezpečnosti a fyzické
bezpečnosti informačních systémů. Úroveň použitých opatření z uvedených oblastí a opatření k zajištění důvěrnosti dat během
přenosu musí odpovídat úrovni požadované pro nejvyšší stupeň utajení utajovaných informací, se kterými informační systém
nakládá.

(3) Bezpečnostní provozní mód s nejvyšší úrovní je takové prostředí, které umožňuje současné zpracování utajovaných
informací klasifikovaných různými stupni utajení, ve kterém všichni uživatelé musí splňovat podmínky pro přístup k utajovaným
informacím nejvyššího stupně utajení, které jsou v informačním systému obsaženy, přičemž všichni uživatelé nemusí být
oprávněni pracovat se všemi utajovanými informacemi. Bezpečnost informačního systému, který je provozován v bezpečnostním
provozním módu s nejvyšší úrovní, se zabezpečuje splněním minimálních bezpečnostních požadavků v oblasti počítačové
bezpečnosti uvedených v § 7 a dále opatřeními z oblasti administrativní a personální bezpečnosti a fyzické bezpečnosti
informačních systémů. Úroveň použitých opatření z uvedených oblastí a opatření k zajištění důvěrnosti dat během přenosu musí
odpovídat úrovni požadované pro nejvyšší stupeň utajení utajovaných informací, se kterými informační systém nakládá.

ZÁKON 412-2005

Vymezení pojmů

Pro účely tohoto zákona se rozumí

a) utajovanou informací informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu
České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu
utajovaných informací (§ 139)

Druhy zajištění ochrany utajovaných informací

Ochrana utajovaných informací je zajišťována

a) personální bezpečností, kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana,
b) průmyslovou bezpečností, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem,
c) administrativní bezpečností, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,
d) fyzickou bezpečností, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,
e) bezpečností informačních nebo komunikačních systémů, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému a
f) kryptografickou ochranou, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací.

Bezpečnost informačních a komunikačních systémů

§ 33a

Státní správu v oblasti ochrany utajovaných informací podle této hlavy vykonává Národní úřad pro kybernetickou a informační bezpečnost, pokud tento zákon nestanoví jinak.

§ 34

Informační systém

(1) Informačním systémem nakládajícím s utajovanými informacemi se pro účely tohoto zákona rozumí jeden nebo více počítačů, jejich programové vybavení, k tomu patřící periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací (dále jen "informační systém").

(2) Informační systém musí být certifikován Národním úřadem pro kybernetickou a informační bezpečnost [§ 46 odst. 1 písm. b)] a písemně schválen do provozu odpovědnou osobou nebo jí pověřenou osobou.

(3) Informační systém podnikatele, který má přístup k utajovaným informacím stupně utajení Vyhrazené, může být schválen do provozu jen v době platnosti prohlášení podnikatele; zánikem platnosti prohlášení podnikatele zaniká též schválení informačního systému do provozu.

(4) Nakládat s utajovanou informací lze pouze v informačním systému splňujícím podmínky podle odstavce 2 nebo 3.

(5) Schválení informačního systému do provozu podle odstavce 2 musí odpovědná osoba nebo jí pověřená osoba písemně oznámit Národnímu úřadu pro kybernetickou a informační bezpečnost do 30 dnů od tohoto schválení.

(6) Prováděcí právní předpis stanoví

a) požadavky na informační systém a podmínky jeho bezpečného provozování v závislosti na stupni utajení utajovaných informací, s nimiž nakládá, a na bezpečnostním provozním módu a

b) obsah bezpečnostní dokumentace informačního systému.