# Ochrana programů a dat

Josef K a ň o v s k ý

## 1. Účel ochrany

Výpočetní technika se stala významným nástrojem pro zpracování informací nejrůznějšího druhu. Po období obdivu k výpočetní technice a také k její ceně, nastává období, kdy již nehledáme hodnoty jen nebo hlavně v prostředcích výpočetní techniky jako takových, ale převážně v informačních hodnotách výpočetní technikou zpracovávaných. Není dnes žádnou výjimkou, kdy informace umístěné v počítači nebo na přenositelném médiu mnohonásobně převyšují jeho hodnotu. Velmi významnou oblastí výpočetní techniky z hodnotového hlediska jsou programy, zvláště univerzálně použitelné. Ačkoliv jsou z obecného pohledu rovněž počítačovými informacemi, zasluhují z hlediska ochrany specifickou pozornost.

Objekty, které se nejčastěji v oblasti výpočetní techniky ochraňují, je možné rozdělit do oblastí:

- lidé
- technika
- data
- programy.

Otázka ochrany lidí z jakéhokoliv hlediska není v další části žádným způsobem diskutována.

Z hlediska metod ochran ve výpočetní technice dále nejsou probírány ochrany právní.

## 2. Klasické ochrany

Klasické ochrany, založené na fyzickém znepřístupnění chráněných objektů, mají ve výpočetní technice své uplatnění. V určitých podmínkách jsou dokonce dominujícími metodami ochrany. Jejich výhodou je dostupnost a zpravidla nízké náklady. Tyto druhy ochran není třeba podrobněji rozvádět, neboť jsou založeny na rozmanitých zabezpečovacích zařízeních jako jsou pečetě, mechanické zámky, připevňování výpočetní techniky k nepřemístitelným předmětům, rozdělování výpočetní techniky na nefunkční části, blokování napájení, trezory, uzamknuté místnosti, elektronické a jiné alarmy, ostraha osobami, organizační opatření atd.

Výhodou klasických ochran je jejich relativní jednoduchost, možnost zajištění osobami, které nejsou znalé oblasti výpočetní techniky. Nevýhoda klasických metod ochrany spočívá v možnosti překonání ochrany za použití jistého stupně násilí.

## 3. Ochrany využívající technických prostředků

Tyto ochrany spočívají převážně na informačních znalostech, které nelze nahradit zpravidla žádným stupněm násilí. Obecně lze konstatovat, že teoreticky neexistuje nepřekonatelná ochrana. Pokud je systém ochrany pomocí technických prostředků důkladně propracován, může zajistit ochranu na takové úrovni, kterou nelze překonat v "rozumném" čase za vynaložení "rozumných" prostředků.

Dále jsou přehledově uvedeny vybrané ochranné techniky, dělené podle chráněných objektů.

### 3.1 Ochrana dat

Ochrana dat zajímá velmi širokou škálu uživatelů. Přitom uživatelé pohlížejí na data z různých zorných úhlů. Jejich požadavky se liší účelem, náklady, stupněm ochrany aj. Některé možnosti jsou dále popsány.

**Ochrana před ztrátou a poškozením**

Základní ochrana před ztrátou a poškozením spočívá nejčastěji v jednoduchém zálohování. Jeho nejjednodušší formou je manuální kopírování. Řada prostředků pro přípravu dat je vybavena automatickým zálohováním, odvozeným od času nebo množství pořízených dat. Tento druh ochrany vyhovuje pro případy zabránění ztrátám dat poruchou, havárií, omylem ap. Předností zálohování je jeho jednoduchost, nevýhodou je nezajištění ochrany dat vzniklých po posledním zálohování.

Nové, zejména síťové systémy, zabývající se bezpečným ukládáním dat mají vyřešeno automatické zálohování dat na dva různé nosiče. Uživatel se pak nemusí o zálohování speciálně starat.

Zvláštním případem ochrany dat před poškozením je požadavek zajistit s vysokou jistotou, aby data při zpracování měla nezměněný tvar vůči předchozímu stavu, tj. možnost ověření jejich úplnosti a původnosti. Nejjednodušším případem pro tuto kontrolu je porovnání se zálohovaným stavem. Další možností je kontrola pomocí redundance, např. podélným součtem. Tento součet nemusí být uchováván z bezpečnostních důvodů společně s daty.

**Ochrana před neúmyslným poškozením**

Při práci s daty na počítači není zcela neobvyklé selhání lidského faktoru. Jednou z účinných metod ochrany před neúmyslným poškozením dat je rovněž zálohování. Mimo to se používá i řada dalších opatření, jejichž cílem je zvýšit pozornost obsluhy. Velmi rozšířené je tzv. potvrzování před rozhodujícím úkonem, který může potencionálně znamenat ztrátu dat, například při vymazávání nebo přepisování souborů. Velmi používané jsou také ochrany proti zápisu realizované buď technickými prostředky (např. zálepka na disketě) nebo programovými prostředky (např. přiřazení atributu "jen čtení").

V jistém smyslu lze do této skupiny prostředků zařadit i nástroje na obnovu poškozených, respektive zrušených dat. K nejpoužívanějším prostředkům patří obnovování zrušených souborů (viz např. funkce Undelete produktu [11] nebo Obnov produktu [3]). U obnovování se využívá skutečnosti, že data souboru nejsou při operaci zrušení fyzicky vymazána, ale soubor je pouze vyřazen z evidenčního seznamu.

Výrobci disketových médií často nabízí obdobné služby pro jejich média poškozená vnějšími vlivy, např. přelomené nebo znečištěné médium ap.

**Ochrana před neoprávněným přístupem**

Cílem tohoto druhu ochrany je zabránit nepovolaným osobám získat datové informace. K tomu se nejčastěji využívá kódování nebo zamezení v přístupu. U kódování je nedůležitější vlastností možnost případného odkódování bez znalosti přístupových práv. Dnes jsou známy algoritmy, které prakticky nedávají možnost provést rozkódování v rozumném čase (např. několik let). Je tedy s podivem, že někteří dodavatelé nabízejí kódovací metody odhalitelné během jednotek hodin. Pomocným kriteriem pro ochranu před neoprávněným přístupem je, zda některá oprávněná osoba může mít zájem předat předat přístupová práva neoprávněné osobě.

K často používaným metodám ochrany dat před neoprávněným přístupem patří ochrana kódováním heslem. Použije-li se kvalitní kódovací algoritmus, který heslo používá jako vstupní parametr ke kódování, může být tato ochrana velmi účinná. Za nekvalitní se považují způsoby ochrany dat heslem, které heslo použijí jen jako překážku ke spuštění jednoho univerzálního algoritmu anebo kódovací algoritmy, které v nějaké formě uloží heslo do výsledných zakódovaných dat; takové způsoby ochrany lze zpravidla snadno překonat laděním kódovacího algoritmu. Ochrana heslem může být dostatečná pro případy, kdy nehrozí prozrazení hesla, tj. osoby, které znají heslo, jsou spolehlivé. Hrozí-li sdělení hesla oprávněnou osobou, je ochrana neúčinná. K další potencionální nevýhodě této ochrany patří ztráta dat při zapomenutí hesla. Příkladem tohoto druhu ochrany je program [13].

Přístup k datům pro omezený počet osob bez nevýhod známých pro utajení heslem lze zajistit pomocí prostředků typu "klíč", který je nenapodobitelný. V utajeném stavu mohou být data zakódovaná některou spolehlivou metodou a k jejich odkódování je třeba použít klíče. Nenapodobitelnost klíče lze založit na technické konstrukci, technologii (např. zákaznický integrovaný obvod) nebo i na nekopírovatelné disketě. Jelikož se kódování opírá o programové algoritmy, je nezbytné tvořit i tyto algoritmy s ohledem na bezpečnost utajovaných dat (algoritmy bez klíče nesmí umožnit odkódování). Tento druh ochrany je vhodný nejen pro ochranu dat v počítači, ale i pro veřejný transport dat (poštou, v počítačové síti ap.). Příklady uvedených prostředků mohou být např. [5] a [2].

V poslední době je za velmi zajímavou oblast ochrany dat považován systém ochrany veřejným klíčem (viz [15]). Tento systém umožňuje šifrovat data klíčem veřejným, ale dešifrování pouze klíčem soukromým. Tato technologie značně usnadňuje výměnu zašifrovaných dat bez nutnosti výměny klíčů. Technologie je rozvíjena několika rozhodujícími světovými počítačovými producenty, avšak zřejmě rozhodujícím okamžikem pro rozšíření bude stanovení amerického standardu.

**Ochrana počítačových systémů**

Chrání-li se počítačové systémy, chrání se tím většinou více data v něm obsažená než samotné technické prostředky. Úroveň a složitost ochrany počítačových systémů se liší zejména sledovaným účelem ochrany počínaje od jednoduchého blokování rozběhu počítače až po složité víceuživatelské systémy s přidělováním řady druhů přístupových práv. Dále jsou uvedeny spíše jednodušší ochrany.

Blokování rozběhu počítačů řady PC dnes již nabízí řada dodavatelů počítačů. Nejčastějším řešením je tzv. Startovací heslo, které je nutno zadat při 1. zapnutí počítače nebo po resetu (umožňuje např. [4]). Není-li počítač pod dohledem, je tím chráněn před přístupem neoprávněné osoby . Neprozradí-li se heslo, je snad jedinou možností přístupu k datům v počítači jen jeho demontáž.

Zajímavou možností k doplnění výše uvedené ochrany v době, kdy je počítač již rozběhnutý, avšak obsluha se potřebuje krátkodobě od počítače vzdálit, je systém pro dočasné zablokování počítače tzv. "horkou klávesou" a jeho opětný rozběh zadáním hesla. Tuto možnost kombinovanou se zadáváním hesla při rozběhu počítače z pevného disku nabízí [7].

Jednoduchou ochranu blokující přístup k počítači, nabízí i zámek klávesnice, často komerčně nabízený s počítačem, nebo jednoduchý program, realizující obdobnou funkci softwarově.

Existuje řada softwarových systémů, které umožňují definovat přístupová práva k počítačovým zdrojům. Tyto systémy například umožňují vymezit různým uživatelům

následující přístupová práva: čtení z diskové jednotky, zápis na diskovou jednotku, spuštění programů, čtení programů, modifikace programů, zápis programů, přímé čtení sektorů, přímý zápis sektorů, ochrana zavedení operačního systému z diskety, kontrola hlavního zavaděče, možnost konfigurace systému podle přístupových práv uživatele ap. (viz. [12]). Slabinu softwarových ochranných systémů, spočívající v možnosti proladění pomocí programů zavedených z diskety, potlačují systémy založené na technických prostředcích. Např. [1] kromě výše uvedených vlastností zahrnuje i přístupová práva práva pro periferie jako jsou paralelní porty, sériové porty, modemy ap. Jeho nadstavba dokonce umožňuje vymezit jednotlivým uživatelům přístupová práva pro vybrané adresáře i soubory.

Speciálním ochranným systémem je [16]. Tento systém zahrnuje kromě zajištění ochrany pomocí přístupových práv ještě také ochranu neoprávněného pohybu systému (ochrana před zcizením, demontáží) pomocí čidla pohybu a zvukového alarmu 90dB.

### 3.2 Ochrana programů

Ochranu programů lze podle účelu dělit do několika skupin.
Významnou skupinu tvoří ochrana vhodná pro uživatele programů a zahrnuje zejména ochranu před poškozením, popř. před neoprávněným používáním. Druhá skupina ochran je určena pro distributory a autory programů a zahrnuje ochranu před neoprávněným kopírováním a ochranu obsahu programů.

**Ochrana programů před poškozením**

Smyslem tohoto druhu ochrany je předcházet spouštění poškozených programů, které mohou způsobit ztrátu dat, programů, případně i poškození počítačové techniky. Z dvou nejznámějších metod ochran prevenční a detekční je první z nich obecně užitečnější, neboť zachycuje potenciální nebezpečí s předstihem.

Jednoduchým preventivním prostředkem pro ochranu programů před poškozením ať už poruchou, osobou nebo virem je systém založený na jeho kontrole před každým spuštěním pomocí kontrolních součtů [14]. Výhodou tohoto systém je, že nezatěžuje obsluhu a provádí ochranu průběžně.

Ochranu programů před poškozením zajišťuje také řada ochranných systémů, řešících přístupová práva. Např. ochranný systém [12] řeší možnost zákazu modifikace nebo vytvoření programu a je tedy schopen rozpoznat, zda nastal pokus o nákazu programu virem nebo zda neoprávněná osoba se pokouší vložit program do počítačového systému. Jeho činnost je však závislá na nastaveném druhu ochrany.

Obdobnou preventivní ochranu poskytuje množství antivirových prostředků, umístěných rezidentně v paměti. Jejich společnou nevýhodou bývá vynucený zásah obsluhy při potřebném zápisu. Naopak vyhledávací a kontrolní antivirové prostředky jsou užitečné až po vniknutí viru do systému. K jejich využití dochází, až se viry projeví svým účinkem, bohužel, často již nenapravitelným. Vyhledávací prostředky mají svou působnost omezenou jen na viry jim známé, což bývá zpravidla zlomek existujících virů.

**Ochrana programů před neoprávněným používáním**

Jde o jednodušší druh ochrany programů před neoprávněnými osobami, pokud je splněn předpoklad, že oprávněné osoby nemají v úmyslu poskytnout program osobám neoprávněným. Není-li splněn, je třeba použít metod ochrany před neoprávněným kopírováním.

Jedním z dostatečně účinných způsobů ochrany programů před neoprávněným používáním je ochrana heslem. Požadavky na kódovací metody jsou obdobné jako u ochrany dat heslem. Příkladem ochranného produktu pro ochranu heslem je [17].

Požadavky na ochranu programů před neoprávněným používáním splňují i ochranné přístupové systémy (viz např. [12] a [1]).

**Ochrana programů před laděním a prohlížením**

Je určena především pro ochranu obsahu programu. Jejím cílem není bránit kopírování. Aby splnila svůj účel, měla by obsahovat antiladící opatření a zakódování chráněného programu. Využívá se pro ochranu unikátních algoritmů a také pro ochranu demonstračních verzí programů. Příkladem tohoto typu ochrany je [10].

**Ochrana programů před neoprávněným kopírováním**

Využívají ji především distributoři a autoři programů, ale také osoby odpovědné za využívání smluvního software ap.

Principiálně má ochrana programů několik článků, které zajišťují nekopírovatelnost pro různé stavy programu. Hlavním, avšak nikoli jediným, článkem ochrany, pokud má být chráněný program komerčně prodáván, je nenapodobitelná substance, jejíž existence je ověřována spouštěným programem. Touto substancí bývá ochranná zástrčka, napojitelná na počítač (zpravidla na sériový nebo paralelní port) nebo nekopírovatelná disketa. Je-li program instalován přímo u uživatele, nemusí ochrana tuto substanci zahrnovat. Další části ochrany je programová část, zajišťující ověření přítomnosti ochrany. Tato část musí u dobré ochrany obsahovat antiladící opatření, aby nebylo jednoduše možné zjistit způsob ověření přítomnosti nekopírovatelné substance a to pak nahradit simulací, případně vytvořit skutečnou

nebo programovou náhražku substance nebo ověřovací části programu. Rovněž nezanedbatelnou částí ochrany je způsob, pestrost a složitost ověřování nenapodobitelné substance. Neméně důležitým kriteriem je četnost výskytu ověřování substance v ochráněném programu a způsob předávání výsledku testu ověření do programu. Existuje mnoho tzv. ochran, které volají ochrannou funkci toliko pomocí volání s navráceným parametrem typu ano/ne. Mnohdy je také důležité, aby se program nevyskytoval v operační paměti jako celek ve funkčním stavu, aby nemohl být z ní zkopírován. Vykazuje-li ochrana programu ve všech stadiích dostatečnou odolnost, teprve pak splní své poslání.

Mezi poměrně levné a rozšířené ochrany programů patří tzv. disketové ochrany, založené na nekopírovatelnosti diskety, která se dosahuje buď nestandardním formátováním (viz [8]) nebo unikátním poškozením magnetického povrchu, např. laserovým paprskem. Druhý způsob je všeobecně považován za nekorektní, s ohledem na podstatu magnetického média (uvolněné velmi tvrdé feritové jehličky nepříznivě působí na čtecí hlavy). Program chráněný disketovou ochranou je pak "vázán" na nekopírovatelnou disketu a ověřuje její přítomnost v disketové mechanice. Nutnost přítomnosti diskety v mechanice poněkud tento druh ochrany handicapuje.

Zdokonalením disketové ochrany je její instalační nadstavba, která umožňuje provést instalaci na počítač. Při instalačním úkonu je prováděno zmapování řady vlastností počítače, tak aby byla pokud možno co nejlépe zajištěna jeho identifikace. Nainstalovaný program pak při své činnosti ověřuje, zda je provozován na počítači, na který byl instalován. Uživatel řádně nainstalovaného programu má u takto chráněného programu pocit, jakoby pracoval s programem neochráněným. Kvalitu ochrany určuje komplexnost zmapování počítače, na který se provádí instalace, nezávislost na konfiguraci počítače a jeho typu ap. Instalační ochrana umožňuje provádět i více instalací z jediné diskety, případně provádět i odinstalace a tím přenášení chráněného programu mezi různými počítači, dále umožňuje i zálohování nainstalovaného programu, instalaci na server sítě aj. (viz [9]). Nízká pořizovací cena dává předpoklad jejího použití i pro programy z nižší cenové kategorie.

Ochrana programů ochrannou zástrčkou (hardlock) je další druh ochrany programů. Její technická podstata umožňuje nabídnout s výjimkou možnosti provozu chráněných programů na více počítačích řadu vlastností navíc ve srovnání s instalační ochranou. Dnešní pokročilé zástrčky nepotřebují žádné napájení, běžně obsahují nonvolatilní paměť, využitelnou pro ochranné evidence a hardwarový kódovací algoritmus (viz [6]). Pokud je dobře navržena jejich softwarová podpora, mají předpoklady být kvalitní ochranou. Pořizovací náklady předurčují jejich využití pro dražší programy.

## 4. Závěr

Uvedený výčet je jen ilustrací aktivit dodavatelů technických ochranných prostředků pro výpočetní techniku. Jeho zaměření bylo určeno k inspiraci a zamyšlení uživatele nad některými potencionálními problémy, vznikajícími s rozmáhající se počítačovou kriminalitou.

## Literatura:


[1] DataLock: MicroDevelopment Corp., USA
[2] Disketový klíč: Golem, Rožnov p. R., ČSFR
[3] DOS Manažer: Golem, Rožnov p, R., ČSFR
[4] DTK-BIOS: DTK Computer Inc., Taiwan
[5] Fast-Eye: FAST GmbH, NSR
[6] HASP: Aladdin K. S., Israel
[7] HD-HESLO: Golem, Rožnov p. R., ČSFR
[8] HRADBA 1, 2 a 2A: Golem, Rožnov p. R., ČSFR
[9] HRADBA 3, 4 a 4A: Golem, Rožnov p. R., ČSFR
[10] HRADBA 5: Golem, Rožnov p. R., ČSFR
[11] PCTools: Central Point Software, Inc., USA
[12] Personal Guardian: LieberLog, Praha, ČSFR
[13] PKZIP: PKWARE, Inc., USA
[14] POJISTKA: Golem, Rožnov p. R., ČSFR
[15] RSA Public Key Cryptosytem: RSA Data Security, Inc., USA
[16] Safegard: Global C.I.S. Ltd, UK
[17] Tajenka: Golem, Rožnov p. R., ČSFR


---


**Autor:** Ing. Josef K a ň o v s k ý
GOLEM, P. O. BOX 66, 756 61 Rožnov p. R.
tel. 0651 - 54044, 544983