# **LICENCE**

Program, který někdo vytvoří, je podle zákona považován za tzv. **AUTORSKÉ DÍLO** a jeho tvůrci (firma, pro kterou pracují) k němu mají **AUTORSKÁ PRÁVA**, podobně jako autoři knih, hudební skladatelé atd.

Z toho plyne, že vy jako uživatelé nemůžete koupit toto dílo jako celek se všemi právy k němu, ale můžete získat pouze **LICENCI** = oprávnění k užívání programu.

Dále z toho plyne, že nesmíte žádným způsobem používat ve svých dílech toto dílo, pokud k tomu autor nedá svůj výslovný souhlas. Licence je někdy nepřenosná, svázaná s určitým počítačem, jindy ji můžete někomu prodat (ale pak už nesmíte program používat).

Koupíte-li program, většinou dostanete krabici, ve které se nachází:

* Vlastní program na nějakém nosiči (CD nebo DVD)
* Licenční ujednání – za jakých podmínek smíte program užívat
* Manuál – návod k jeho užívání

Při instalaci programu většinou musíte odsouhlasit **LICENČNÍ SMLOUVU** s koncovým uživatelem (tzv. EULA – End User License Agreement). Tím dáváte najevo svůj souhlas s licenčním ujednáním.

Licenční smlouva je typem obchodní smlouvy, je tedy podřízena zákonu. Kontrolu legálnosti softwaru provádí specializované oddělení Policie ČR. Žádná jiná organizace nemá právo občany kontrolovat.

**OCHRANA PROGRAMŮ PŘED NELEGÁLNÍM KOPÍROVÁNÍM**

Výrobci programů chrání své programy tak, že se snaží kopírování přímo znemožnit nebo aspoň používají prvky, které usnadní usvědčení pachatele:

* **LICENČNÍ (SÉRIOVÉ) ČÍSLO** – Program při instalaci vyžaduje zadání licenčního čísla, bez kterého nelze instalaci dokončit. Dodavatelská firma má evidenci sériových čísel a uživatelů.
* **AKTIVACE PŘES INTERNET NEBO TELEFON** – Program po instalaci vyžaduje aktivaci přes Internet nebo telefon. Po aktivaci je svázáno určité licenční číslo s určitým počítačem.
* **HARDWAROVÝ KLÍČ** – Je to malé zařízení, které se připojuje většinou k USB portu počítače. Bez něj program nefunguje. Je to velmi bezpečná ochrana. Používá se u nejdražších skupin programů.
* **CHYBOVÁ MÍSTA NA DISKU** – Disk s programem nelze jednoduše zkopírovat. Většinou obsahuje speciálně upravená chybná místa, která způsobí chybu při kopírování.

Překonávání těchto ochran je nelegální.

Nejčastěji používané druhy licencí:

* **OEM SOFTWARE** – Jsou to normální nové verze programů, které jsou však nabízeny pouze současně s novým hardwarem za sníženou cenu (někdy až na třetinu běžné ceny). OEM programy jsou však vázány na díl, se kterým byly zakoupeny (u PC je to základní deska), nedají se instalovat na jiný počítač. A nedá se z nich upgradovat na vyšší verzi programu.
* **KOMERČNÍ VERZE PROGRAMŮ** – Majitelé komerčních programů poskytují koncovým uživatelům za úhradu licenci k užívání těchto programů.
* **DEMOVERZE PROGRAMŮ** – Demoverze jsou programy, které mají zablokované některé funkce, často ukládání souborů na disk a tisk. Dodávají se zdarma nebo za malý poplatek. V demoverzi si vyzkoušíte funkčnost a ovládání programu a pak se rozhodnete, zda program koupíte nebo ne.
* **ZKUŠEBNÍ (TRIAL) VERZE** – Ty většinou umožňují plnohodnotnou práci, ale jen po určitou dobu. Po uplynutí této doby program nelze spustit ani znovu nainstalovat.
* **SHAREWARE** – Takovýto program si můžete nainstalovat, pracovat s ním a po určité době jste povinni zaslat jeho autorovi uvedený poplatek (tzv. registrační poplatek). Na základě registračního poplatku pak smíte program legálně užívat, a navíc vám jeho autor často pošle stručný manuál, případně i novou verzi programu.
* **FREEWARE** – Program, označený jako freeware, můžete používat a rozšiřovat zdarma, požaduje se jen dodržování autorských práv (licence k programu je poskytována zdarma). Nesmí se tedy zahrnovat do komerčně šířených programů a nesmí být změněn.
* **PUBLIC DOMAIN** – Je to skupina programů k volnému užití. Tyto programy lze používat, volně šířit i upravovat. Autoři se vzdávají některých svých práv k programu a nechají uživatele s ním nakládat podle libosti.
* **OPEN SOURCE A LICENCE GPL** – Open Source znamená doslova otevřený zdroj. Takové programy musí být vždy šířeny i s uvedením zdrojových textů, takže každý může přesně zjistit, jak takový program funguje. Každý ho také může vylepšit, opravit v něm chybu, použít ho ve svém programu, vždy však musí takový produkt opět distribuovat jako Open Source. Přesné podmínky pak stanovuje licence GPL (General Public Licence – všeobecná veřejná licence). Nejrozšířenější takovou licencí je GNU/GPL.

## **AUTORSKÉ PRÁVO**

V předchozí části jsme si řekli, že program je považován za AUTORSKÉ DÍLO a jeho použití se řídí AUTORSKÝM ZÁKONEM. Nyní se budeme věnovat dalším autorským dílům (textům, obrázkům, hudbě a videu) a možnostem jejich použití v našich dokumentech. Použití cizích autorských děl pro vlastní materiály se věnuje paragraf Autorského zákona s nadpisem **CITACE**.

Z něj plyne pro **text** následující:

* Pokud užíváme díla při výuce ve škole (tj. výlučně k vyučovacím účelům), můžeme užít celé dílo.
* Pokud vytvoříme dokument (prezentaci, text), který umístíme na web, jedná se o zveřejnění samostatného díla a cizí díla můžeme použít pouze v odůvodněné míře. Co je tato míra, zákon nespecifikuje. Vždy musíme uvést **jméno autora**, název díla a pramen.

**Obrázky** používáme vždy celé. Můžeme je tedy bez ohledu na práva autora užívat pouze pro vyučovací účely.

**Obrázky** v dílech, která zveřejníme je možné použít:

* Své vlastní kresby či fotografie (pozor na práva osob a značek).
* Z volně dostupných zdrojů, u kterých je užití výslovně povoleno.
* Po zajištění souhlasu autora, případně majitele autorských práv.

**Hudbu a video** můžete získat a užít pro osobní potřebu. Pro svou osobní potřebu můžete také zhotovit záznam, rozmnoženinu nebo napodobeninu díla. Nesmíte je ale šířit, a to ani zdarma. Zakázaná je také veřejná produkce.

## **ANTIVIROVÁ OCHRANA**

**Bezpečný počítač** pro práci je takový počítač, který neobsahuje žádný nežádoucí software a který není napadnutelný z Internetu. Část bezpečnosti zajišťují technická opatření, velký podíl mají také naše znalosti a naše opatrnost.

V programech se mohou objevit **bezpečnostní chyby** (díry). Škodlivé kódy (viry) tyto chyby využívají k tomu, aby se dostali do našeho počítače. Výrobci programů vydají opravu (záplatu, patch), která chybu odstraňuje, musíme ji však do programu na našem počítači aplikovat – **aktualizovat program**. Abychom nemuseli aktualizace hlídat, je dobré mít nastavené automatické aktualizace.

Pozn.: Při nákupu operačního systému je na instalačním CD často napsáno: včetně **service pack**. Servisní balíčky obsahují veškeré v době jejich vzniku známé záplaty a často i nové funkce a vylepšení zabezpečení počítače.

Každý počítač připojený k Internetu má svoji jednoznačnou IP adresu. Jednotlivé služby (web, pošta, sdílení souborů) pak využívají jednotlivé **porty**, jakési brány do počítače. Portů je teoreticky 65535 a přes všechny by se do počítače mohly dostat počítačové červy. Využívají je také lidé, snažící se o neoprávněný přístup do cizích systémů (**hackeři**). Program, který hlídá, co se na jednotlivých portech děje, a povoluje jen námi vyžádanou komunikaci, se nazývá **FIREWALL**.

* **OSOBNÍ FIREWALL** je dnes většinou součástí operačního systému, kontroluje síťovou komunikaci z/do počítače.
* **SÍŤOVÝ FIREWALL** sleduje komunikaci mezi vnitřní (lokální) sítí a vnější sítí (Internetem). Bývá součástí směrovače (routeru).

**MALWARE** je škodlivý kód, který někdo vytvořil, aby získal důvěrná data z vašeho počítače, získal kontrolu nad vaším počítačem nebo aby zničil vaši práci.

* **VIRUS** je malý program, který se umí vložit do jiného programu a s ním se šířit. Spuštěním programu tedy spustíte i virus, který napadne další programy.
* **MAKROVIRUS** je virus, který není součástí programu, ale dokumentu, který může obsahovat makra, to jsou vlastně v dokumentu vložené programové kódy.
* **ČERV** má vlastní soubor a většinou se snaží přimět uživatele počítače, aby ho spustil, případně využívá bezpečnostní chybu a snaží se spustit sám. Některé internetové červy využívají chyby v zabezpečení síťového připojení operačního systému a šíří se přímo v paketech síťového protokolu. Jsou velmi nebezpečné, protože je nezachytí antivirový program a protože nevyžadují k napadení počítače aktivitu uživatele (jen opomenutí instalace aktualizací).
* **ROOTKIT** je škodlivý kód, který běží v jádru operačního systému s právy administrátora počítače. Špatně se detekuje a odstraňuje, protože je součástí jádra operačního systému, může se skrýt před běžným antivirovým programem.
* **SPYWARE** jsou programy, které sledují činnost uživatele a předávají o ní někomu zprávy, nebo prohledávají obsah počítače a opět o něm někoho informují.
* **ADWARE** také sleduje aktivity uživatele počítače na Internetu a cíleně mu zobrazuje reklamu. Nemusí to být vždy škodlivý kód.

Virus (červ), který přijde na váš počítač, ihned nepoznáte. Nějakou dobu se jen šíří, infikuje další soubory v počítači, rozesílá se na všechny nebo pouze na vybrané e-mailové adresy z vašeho adresáře. Teprve po určité době, v určitý den, po určitém počtu spuštění apod. provede nějakou nepříjemnou činnost:

* **OVLÁDNUTÍ POČÍTAČE** – Program typu **BACKDOOR** otevře některé porty počítače a naslouchá na nich povelům zvenčí. Podobně pracuje **TROJSKÝ KŮŇ**, program, který kromě své zjevné činnosti vykonává ještě nikde neuvedené akce bez souhlasu uživatele. Umožní tak získat útočníkovi přístup do počítače a pracovat s ním.
* **ODCIZENÍ OBSAHU POČÍTAČE** – Vzdálený útočník si může díky získanému přístupu kopírovat soubory z napadeného počítače, případně použít program typu **KEYLOGGER** ke sledování stisknutých kláves (např. při vyplňování políček ve formulářích), nebo **DATAMINDER**, program, který shromažďuje data o činnosti uživatele počítače.
* **VYUŽITÍ POČÍTAČE PRO NELEGÁLNÍ ČINNOST** – Vzdálený útočník přemění nezabezpečený počítač v server rozesílající spam nebo poskytující stránky s nelegálním obsahem.
* **MAZÁNÍ OBSAHU POČÍTAČE** – To již dnes není u škodlivých kódů obvyklé. Kromě uspokojení z poškození neznámého člověka totiž nepřináší žádný finanční efekt.

Škodlivý kód se do našeho počítače dostane nejčastěji přes webové stránky a elektronickou poštu.

## **ANTIVIROVÝ PROGRAM**

Na antivirový program mnoho uživatelů počítače spoléhá jako na nepřekonatelnou ochranu svého počítače. Největším nebezpečím pro počítač však bývá jeho uživatel. Antivir však nabízí hodně a měl by být proto na každém počítači.

* Antivir stále běží v paměti počítače a **kontroluje spouštěné programy a každý otevíraný dokument**. To je nejdůležitější funkce, která by měla zabránit spuštění jakéhokoliv škodlivého kódu.
* Antivir **na náš pokyn otestuje počítač**, přesněji zkontroluje, zda v paměti počítače neběží škodlivý kód a potom zkontroluje všechny (nebo určené) soubory v počítači.

Jak funguje antivirový program:

* **Porovnává programy** se svojí databází škodlivých kódů. Podobně **porovnává adresy webů** s černou listinou nebezpečných stránek.
* **Sleduje podezřelé aktivity** jako je zápis do systémových souborů a jiných programů, na webu obsah programu vloženého do stránky. Má tak šanci nalézt i dosud neznámý vir.

**Aktualizace antiviru** je samozřejmě zcela nutná, jinak by neznal nejnovější hrozby. Všechny antiviry se aktualizují samy, některé i několikrát denně.

**Odvirování nakaženého počítače** není vždy jednoduché, mnoho virů se dokáže skrýt před antivirovým programem. Řešením je nabootovat jiný operační systém z Live CD nebo z USB disku. Vir pak již není aktivní a je možné ho skenováním disku najít a odstranit. Alternativou je vyjmutí disku z nakaženého počítače, jeho umístění v čistém stroji a odvirování.