Vírusy

Vírus je malý, relatívne jednoduchý program, ktorý je schopný sa sám šíriť a vykonáva činnosť, pre ktorú bol napísaný. Terminológia je veľmi podobná tej, ktorá sa používa pri biologickom víruse, práve pre svoju podobnosť. Neoprávnený vstup do systému, jeho modifikácia, získavanie a poškodzovanie cudzích údajov sa označuje pojmom *počítačová infiltrácia*. Proces šírenia vírusu sa označuje ako nákaza alebo *infekcia*. Napadnutý súbor sa označuje ako *hostiteľ* a jeho stav – *infikovaný*. Uchovanie napadnutého súboru bez odstránenia vírusu sa označuje pojmom *karanténa.* Odstráneniu vírusu hovoríme *liečenie*, po úspešnom odstránení je súbor vyliečený.

# Rozdelenie vírusov:

* podľa miesta, kam sa vírusy ukladajú
* podľa spôsobu umiestnenia v pamäti
* podľa spôsobu deštruktívnosti
* podľa schopností maskovať sa pred antivírusovým programom

# Podľa miesta, kam sa vírusy ukladajú:

* + spustiteľné súbory – ako prvý sa otvorí vírus a až potom program, prípadne prepíše začiatok súboru
	+ systémové oblasti – umiestni sa do bootsektora, spustí sa pred OS
	+ dokumenty, ktoré obsahujú makrá
	+ ľubovoľné miesto na disku

# Podľa spôsobu umiestnenia v pamäti:

* + nerezidentné – spúšťajú sa pomocou spustiteľného programu, nakazia aj iné
	+ rezidentné – po spustení napadnutého súboru natrvalo uložia v pamäti a sledujú používateľa

# Podľa spôsobu deštruktívnosti:

* + nedeštruktívne – vizuálne a akustické prejavy
	+ vírusy napádajúce programy – prepisujú program
	+ vírusy ničiace údaje – prekódujú, naformátujú, vymažú
	+ vírusy modifikujúce údaje – občas zmenia údaj
	+ vírusy odosielajúce z PC údaje – pomocou emailov alebo siete
	+ vírusy ničiace HW PC – umožňuje zápis do BIOSu

# Podľa schopností maskovať sa pred antivírusovým programom

* + vírusy, ktorých všetky kópie majú rovnaký kód
	+ polymorfné – pri rozmnožovaní menia kód svojho tela
	+ stealth – maskujú činnosť, skrývajú stopy

# Malware – pokračovatelia vírusov:

* + trójske kone – tvári sa ako žiadaný a neškodný softvér, no v skutočnosti sleduje činnosť používateľa, odosiela údaje a v nečakanej chvíli zaútočí
	+ počítačové červy
		- sieťový červ – šíri sa vďaka chybám v serverových častiach
		- e-mailový červ – šíri sa cez e-maily
	+ spammery – napadnutý PC sa stáva odosielateľom spamu

# Šírenie vírusov:

* + infikovanie prostredníctvom výmenných médií
	+ infikovanie prostredníctvom počítačovej siete
	+ šírenie prostredníctvom e-mailu

# Prejavy vírusov:

* + obťažujúce
	+ deštruktívne

# Prevencia:

* + *pasívna ochrana:*
		- používať legálny SW
		- nepoužívať cudzie pamäťové médiá
		- pravidelne aktualizovať OS a aplikácie
		- minimálne zdieľanie priečinkov
		- používať firewall
		- neotvárať spam, e-mail od neznámych
		- nenavštevovať stránky s pochybným obsahom
		- neinštalovať neznáme programy
		- zálohovať
	+ *aktívna ochrana:*
		- antivírusové programy
		- programy na detekciu malware – identifikujú spyware, adware

**Použitá literatúra**

Skalka, J. – Klimeš, C. – Lovászová, G. – Švec, P.: Informatika na maturity a prijímacie skúšky, Enigma Publishing, 2017, ISBN 978-80-89132-49-2