$\alpha + \omega$, 2003, Nr. 1, 93–99

Antivirusinė programa „Dr.Web" Lietuvos mokykloms

Viktoras Dagys, Rūta Simanavičienė
ims.antivirus@ktl.mii.lt

Straipsnyje aprašoma antivirusinė programa „Dr.Web", kuri nemokamai gali būti naudojama Lietuvos valstybinėse mokymo įstaigose.

Kompiuterių virusas — tai programa, atliekanti tam tikrus veiksmus be kompiuterio vartotojo žinios. Ši programa keičia kompiuteryje esančią informaciją: ją ištrina, įrašo naujos informacijos, modifikuoja vartotojo programas įterpdama į jas savo kopijas. Virusai — tai nedidelės apimties programos, kurios gali „prikibti" prie kitų programų (jas užkrėsti), taip pat atlikti įvairius nepageidaujamus veiksmus bylose. Kompiuterių viruso terminą 1984 metais pasiūlė Fredas Koenas (*Fred Cohen*, žr. http://all.net).

Kompiuterių virusų atsiradimas siejamas su programuotojų sugalvotu žaidimu „Core war" (karas atmintinėje), kurio metu kompiuterio atmintinėje rungiasi dvi programos ir stengiasi užimti kuo daugiau vietos. Jos taip pat ieško priešininko programos ir bando ją ištrinti. Kaip ir kitose srityse, čia sukauptas patyrimas panaudotas ne tik geriems, bet ir blogiems tikslams. Atsirado mėgėjų nevykusiai papokštauti, atkeršyti už neteisėtai nukopijuotas programas arba tiesiog parodyti, ką jie gali. Toks piktybinis kompiuterių virusų platinimas padaro daug žalos, nes asmeniniai kompiuteriai turi gana menkas apsaugos nuo jų priemones.

Saugantis nuo kompiuterių virusų galima daryti svarbių bylų kopijas ir laikyti išoriniuose kaupikliuose, nesinaudoti nelicencijuotomis programomis ir pan. Tačiau šiais laikais kiekvienas dirbantis kompiuteriu naudojasi ir internetu, ir elektroniniu paštu. Parsisiųsdinant įvairias programas, atveriant elektroninius laiškus ar prie jų prikabintas bylas, galima labai nesunkiai į savo kompiuterį paleisti virusą, jeigu tos bylos buvo užkrėstos. Tad atsarginės kopijos ir licencijuotos programos nuo virusų neapsaugos. Būtina naudotis antivirusinėmis programomis, kurios aptinka ir sunaikina virusą bei atstato pažeistas bylas.

Antivirusinių programų savybės

Antivirusinės priemonės įvairiai klasifikuojamos: yra tikrinimo, diskų peržiūros, budinčios, vakcinavimo ir kitos programos.

Tikrinimo programa skirta aptikti ir sunaikinti kompiuterių virusus. Paprastai tokios programos turi virusų, kuriuos jos geba atpažinti, duomenų bazes. Be to, šiuolaikiškose tikrinimo programose esama ir euristinio analizatoriaus, kuris gali aptikti net tuos virusus, kurių aprašų tikrinimo programos duomenų bazėse nėra.

Budinti programa — tai techninė ir programinė įranga, skirta duomenų bei sisteminių disko sričių apsaugai nuo neteisėtų modifikacijų. Jei tai yra techninė priemonė, tai šis komponentas paprastai įmontuojamas kompiuterio magistralėje.

Nerezidentinė vakcina — tai programa, kuri modifikuoja bylą ar kelties sektorių siekdama užkirsti kelią kompiuterių virusui ar jį aptikti. Vakcinacija gali būti nukreipta prieš konkretų virusą

(pavyzdžiui, taip pakeisti bylą, kad virusui atrodytų, jog ši byla jau užkrėsta) arba prieš bet kurį virusą. Pastaruoju atveju vakcina turi gebėti atpažinti ir pranešti apie vakcinuotų objektų modifikaciją. Kartais vakcinos gali net išgydyti užkrėstus objektus.

Rezidentinė vakcina — tai rezidentinė programa, kuri imituoja sistemos užkrėtimą konkrečiu virusu ir tokiu būdu užkerta kelią tikram užkrėtimui. Skirtingai nuo nerezidentinių, rezidentinė vakcina veikia ne konkretų objektą (bylą ar kelties sektorių), o pačią operacinę aplinką (terpę, kurioje virusas plinta).

Norėtųsi turėti vieną programą, galinčią atlikti daugumą išvardytų funkcijų ir kartu budėti kompiuteryje, saugoti jį nuo virusų ir be vartotojo pagalbos su aptiktais virusais susidoroti. Būtent tokias savybes turi antivirusinė programa „Dr.Web".

Matematikos ir informatikos institutas 2002 metais sudarė sutartį su bendrove „Dialogue Science" (http://www.dials.ru/) ir įgijo teisę lokalizuoti bei nemokamai platinti „Dr.Web" programos komplektą visoms Lietuvos valstybinėms mokymo įstaigoms naudojimuisi nekomerciniais tikslais.

Parengtas lokalizuotas „Dr.Web" rinkinys, kurį sudaro trys programos:

- „Dr.Web" — „Windows" 95/98/Me/NT/2000/XP sistemai su grafine sąsaja ir rezidentine programa — virusų filtru „SpIDer Guard";
- „Dr.Web" — „Windows" 95/98/Me/NT/2000/XP sistemoms su komandinės eilutės sąsaja;
- „Dr.Web" — DOS/386 sistemai su komandinės eilutės sąsaja.

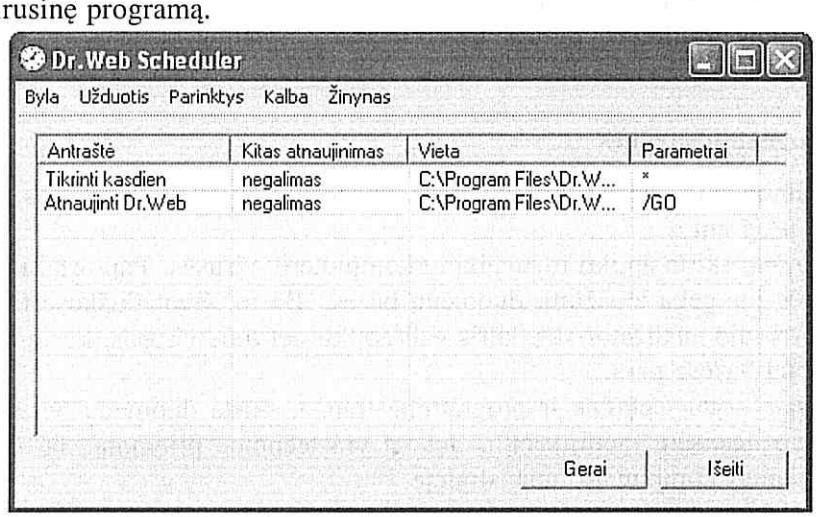
„Dr.Web" programos sandara

Antivirusinė programa „Dr.Web" skirta „Windows" sistemai — tai antivirusinės peržvalgos programos „Doctor Web" ir rezidentinės budinčios programos „SpIDer Guard" kombinacija, kuri įdiegta integruojasi į operacinę sistemą.

Budinti programa „SpIDer Guard" perima kreipinius į bylas ir diskų sistemines sritis ir greit patikrina, ar nėra virusų pavojaus. Programa randa ir nukenksmina visų tipų virusus (kelties, bylų, makrokomandų, HTML ir kt.), tikrina pašto paketus ir pakuotąsias (suglaudintas) bylas, tikrina pagrindinę (operatyviąją) atmintinę ir šalina iš jos virusus.

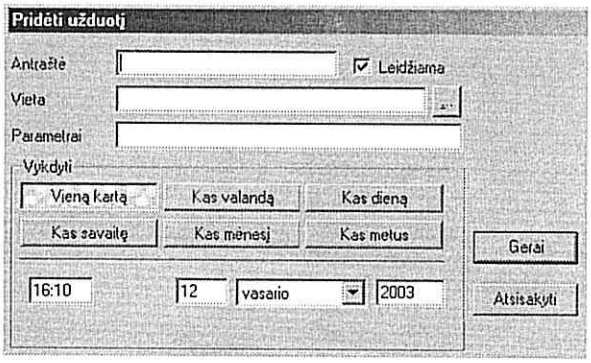
Skirtingai nuo peržvalgos programos „Doctor Web", budinti „SpIDer Guard" viską tikrina automatiškai, t. y. be vartotojo atskiro nurodymo.

„Dr.Web" programa su grafine sąsaja turi specialią programėlę, vadinamą „Dr.Web" planuokliu (1 pav.). Tai nesudėtingas kalendorius, leidžiantis suplanuoti, kada automatiškai paleisti bei atnaujinti antivirusinę programą.



1 pav. „Dr.Web" programos planuoklio pagrindinis langas

„Dr.Web“ planuokliu galima tvarkyti vadinamąsias užduotis. Kiekviena užduotimi aprašoma, kada, kaip ir kurią programą paleisti. Remdamasis šiuo aprašu planuoklis paleidžia programą, be to, galima peržiūrėti užduočių sąrašą, kurti bei šalinti užduotis. Galima keisti užduoties aprašą ir leisti arba neleisti aprašytas užduotis atlikti. Taip pat galima laikinai sustabdyti užduotį (neištrinant jos iš sąrašo).



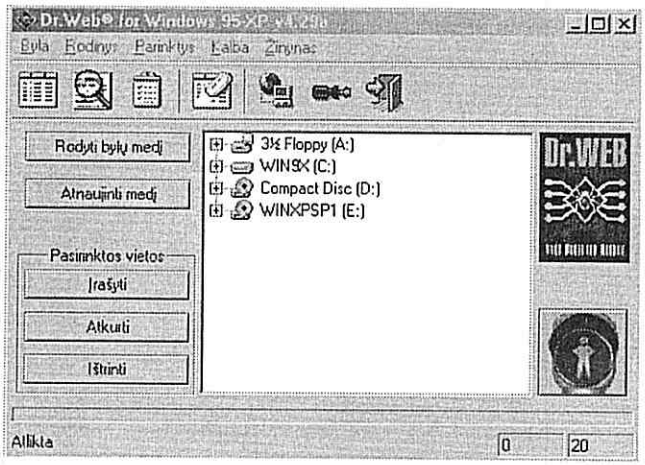
2 pav. Užduoties sudarymo skydelis

Reikiamą „Dr.Web“ rinkinio programą galima parsisiųsdinti iš jai skirto lietuviško tinklalapio (http://aldona.mii.lt/pms/lok/drweb/). Ten pateikti ir naudojimosi šia programa pradmenys.

Atkreipiame dėmesį, kad sėkmingai „Dr.Web“ įdiegti galima tik tada, kai jūsų kompiuteryje nėra kitų antivirusinių programų. Bandant vienu metu naudotis dviem antivirusinėmis programomis, gali kilti įvairių problemų.

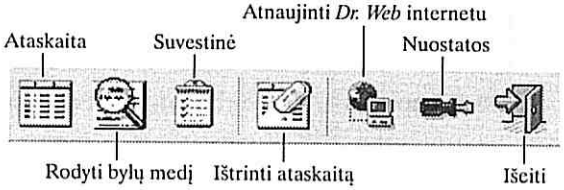
Pagrindinis programos langas

Antivirusinės programos „Dr.Web“ pagrindinį langą matome 3 paveiksle.



3 pav. Pagrindinis „Dr.Web“ programos langas

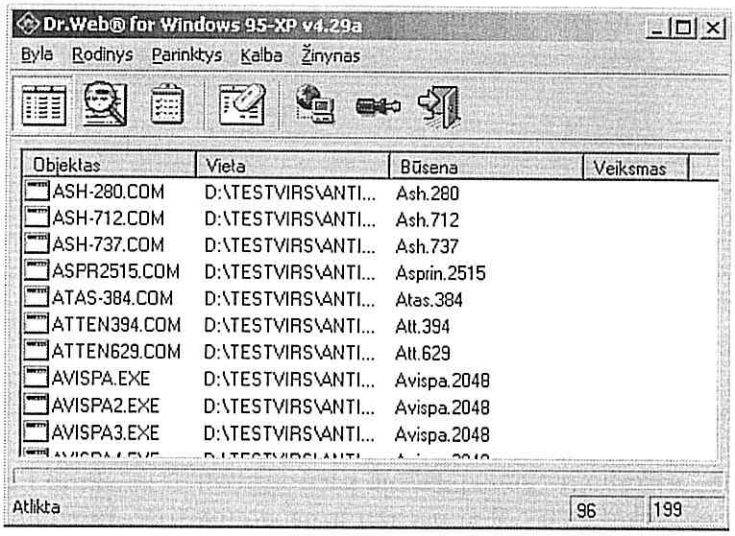
Pirmiausiai susipažinsime su šiame lange esančios programos priemonių juostos mygtukais (4 pav.).



4 pav. „Dr.Web“ programos mygtukų juosta

$\alpha + \omega$

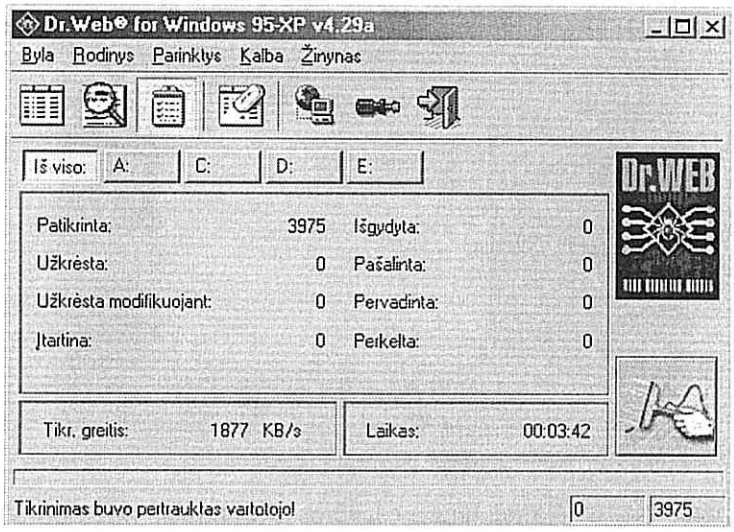
Paspaudę mygtuką *Ataskaita*, išvystame tikrinimo ataskaitą (5 pav.) — informaciją apie užkrėstas bylas, jų vietą, viruso būseną ir kas su ta byla buvo daroma.



5 pav. Tikrinimo ataskaitos langas

Paspaudę mygtuką *Rodyti bylų medį*, matome tokį pat vaizdą, kaip ir ką tik paleidę šią programą (3 pav.).

Paspaudę mygtuką *Suvestinė*, ekrane pamatysime tikrinimo suvestinę (6 pav.) — kiek bylų tikrinta, kiek užkrėsta, kiek išgydyta ir t. t.

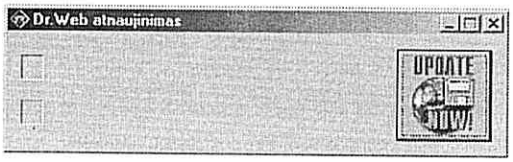


6 pav. Tikrinimo suvestinės langas

Galima gauti atskirai kiekvieno kompiuterio disko tikrinimo suvestinę — tam tereikia paspausti atitinkamą mygtuką. Paspaudus mygtuką , suvestinė išvaloma. Lango apačioje rodomas tikrinimo greitis ir laikas.

Paspaudus mygtuką *Ištrinti ataskaitą*, pašalinama vėliausio tikrinimo ataskaita.

Mygtuku *Atnaujinti Dr.Web internetu* iškviečiama programos atnaujinimo internetu skydelis (7 pav.). Antivirusinės programos atnaujinimo procesas pradedamas paspaudus mygtuką *Update Now!*



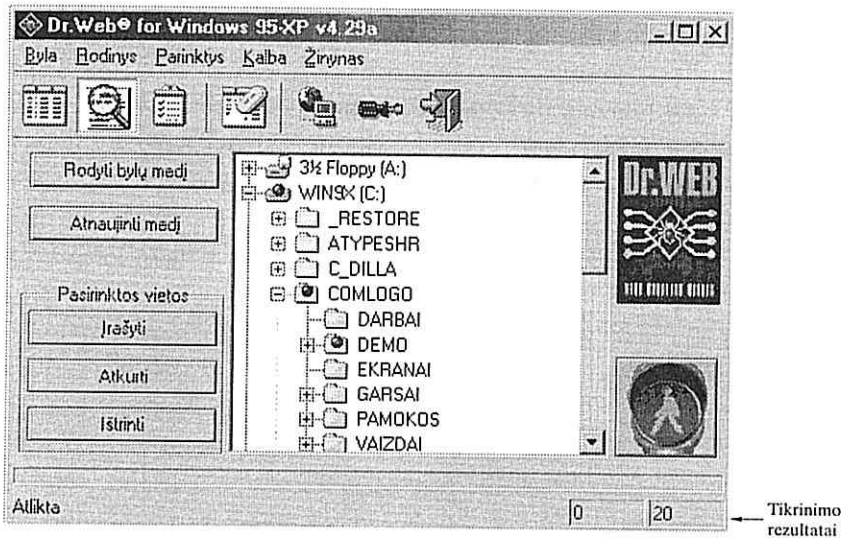
7 pav. „Dr.Web" programos atnaujinimo skydelis

Paspaudus mygtuką *Nuostatos*, iškviečiamas „Dr.Web" programos nuostatų langas. Jį galima išsikviesti ir kitaip: meniu grupėje *Parinktys* pasirinkti *Keisti nuostatas* arba paspausti klaviatūros klavišą F9. Apie šio lango paskirtį rašoma programos nuostatų skyrelyje.

Paspaudus mygtuką *Išeiti*, užveriamas „Dr.Web" programos langas. Tačiau jeigu programa tuo metu tikrina atmintinę ar bylas, programos užverti negalėsime, kol viskas nebus patikrinta arba kol nenutrauksite tikrinimo.

Virusų paieška

Paleidus antivirusinę programą „Dr.Web", ji iš karto patikrina kompiuterio atmintinę ir tuomet lango apačioje (8 pav.) galima pamatyti tikrinimo rezultatus.



8 pav. Tikrinimui pasirinkto katalogo vaizdas

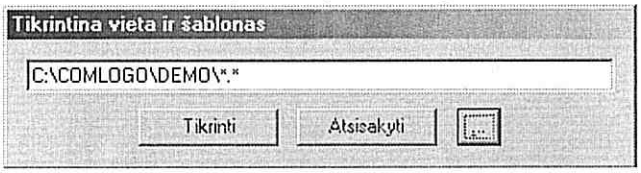
Pirmasis skaičius (0) rodo, kiek užkrėstų bylų yra atmintinėje, antrasis (20) — kiek bylų patikrinta.

Galima patikrinti visą diską, tačiau galima pasirinkti konkrečią disko vietą — katalogą. Norint tikrinti visą diską, reikia medžio lange spragtelėti norimą diską ir paspausti tikrinimą paleidžiantį žalio šviesoforo pavidalo mygtuką. Tikrinant konkretų katalogą, reikia pele spragtelti pliuso ženklelį ties reikiamu disku, paskui ties reikiamu katalogu ir t. t., kol pasiekiamas tas pakatalogis, kurio bylas reikia patikrinti.

Grįžti į pagrindinį programos langą galima paspaudus mygtuką *Rodyti bylų medį*.

$\alpha + \omega$

Kitas konkretaus katalogo tikrinimo būdas: bylų medžio lange spragtelėjus dešiniuoju pelės klavišu, atsiranda tikrintinos vietos nustatymo skydelis (9 pav.).



9 pav. Tikrintinos vietos ir šablono nustatymo skydelis

Paspaudus mygtuką [...], galima pasirinkti, kurio disko, kurį katalogą ar pakatalogį tikrinti. Šią tikrintiną vietą ir šabloną galima išsikviesti paspaudus klaviatūros klavišą F5 arba meniu pasirinkus *Byla* → *Tikrintina vieta.*

Programos nuostatos

Antivirusinės programos „Dr.Web" atliekami veiksmai sugrupuoti ir pateikti penkiose meniu grupėse: *Byla, Rodinys, Parinktys, Kalba, Žinynas* (3 pav.). Trumpai aptarsime kiekvieną grupę.

Meniu grupė *Byla* skirta konkretiems programos veiksmams: paleisti programą (*Pradėti tikrinimą*), nutraukti tikrinimą (*Užbaigti tikrinimą*), pasirinkti tikrintiną vietą ir šabloną (*Tikrintina vieta*), paleisti atmintinės tikrinimą (*Tikrinti atmintinę*), išvalyti tikrinimo ataskaitą (*Ištrinti ataskaitą*), užverti programos langą (*Išeiti*).

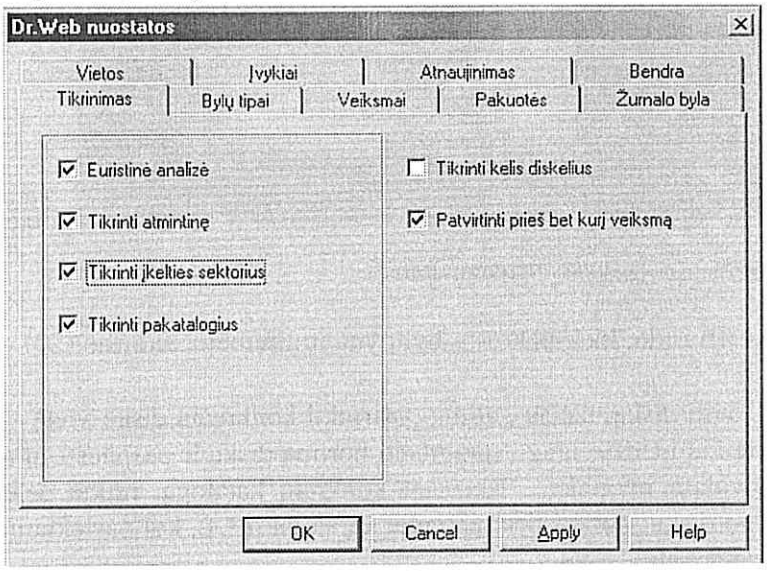
Meniu grupėje *Rodinys* galima pasirinkti, kurį programos langą atverti: *Ataskaitos, Bylų medžio* ar *Suvestinės.*

Meniu grupėje *Kalba* galima pasirinkti, kuria kalba norite matyti visus programos užrašus: anglų ar lietuvių.

Meniu grupėje *Žinynas* galima rasti informacijos apie programos autorius, jos veikimą, licencijos parametrus, reikiamus adresus (*Apie...*) bei terminų žodynėlį (*Žinyno temos*).

Meniu grupę *Parinktys* sudaro keturios komandos: *Keisti nuostatas, Išsaugoti nuostatas, Atkurti nuostatas* ir *Atnaujinimas.*

Išsamiau aptarsime komandą *Keisti nuostatas* (F9). Programa leidžia pasirinkti tokias programos nuostatas, kokių nori vartotojas.



10 pav. Programos nuostatų langas

Nuostatų lange (10 pav.) yra devynios kortelės:

1. *Tikrinimas* — galima nurodyti pagrindines tikrinimo nuostatas.
2. *Bylų tipai* — galima pasirinkti, kokio tipo bylas tikrinti ir tikrinimo veikseną.
3. *Veiksmai* — galima pasirinkti veiksmus, atliekamus su užkrėstais, neišgydomais ir įtartinais objektais: *pranešti, gydyti, šalinti, pervadinti, perkelti į*. Kiekvieno tipo objektams galima pasirinkti tik po vieną veiksmą.
4. *Pakuotės* — pasirenkama, ką programa turės atlikti esant užkrėstoms pakuotėms, užkrėstam paštui ar užkrėstoms talpykloms.
5. *Žurnalo byla* — numatyta byla, kuri bus naudojama žurnalui. Šioje byloje bus įrašoma, kiek užkrėstų bylų rasta, išgydyta, kiek pašalinta ir t. t.
6. *Vietos* — galima nurodyti virusų bazių ir netikrintinų aplankų vietą.
7. *Įvykiai* — po kiekvieno programos veiksmo — *įspėjimo, išgydžius, pašalinus, pervadinus, perkėlus, baigus, įvykus klaidai* — galima nustatyti atitinkamą garsinį signalą. Įdiegus programą jau būna numatyti garsiniai signalai, tačiau kiekvienas vartotojas juos gali pasikeisti savais (t. y. garsinėmis bylomis **.wav*).
8. *Atnaujinimas* — mums svarbus yra tik atnaujinimo adresas, kitos šios kortelės parinktys nekomercinių įstaigų vartotojams nereikalingos.
9. *Bendra* — čia galima pasirinkti tikrinimo prioritetą, nurodyti, ar programai baigiant darbą įrašyti nuostatas.

Baigiamosios pastabos

Diegiant antivirusinę programą „Dr.Web“ operacinėse sistemose „Windows 9x“, „Windows Me“, „Windows 2000“, paprastai pasirenkamas *tipinis* diegimo variantas, o „Windows NT“ bei „Windows XP“ vartotojams patariama rinktis *numatomąjį* — tuomet rezidentinė programa „SpIDer Guard“ tikrai atsiranda darbalaukio užduočių juostoje.

Svarbu žinoti, jog nėra programų, garantuojančių šimtaprocentinę apsaugą nuo virusų. Juk bet kurios antivirusinės programos algoritmui teoriškai visada galima sukurti kontralgoritmą (t. y. virusą), kurio neaptiks konkreti antivirusinė programa. Visa laimė, kad teisingas ir atvirkštinis teiginys: bet kuriam viruso algoritmui visada galima sukurti antivirusinę programą. Remdamasis baigtinių automatų teorija tai įrodė straipsnio pradžioje jau minėtas Fredas Koenas.

„Dr.Web“ programa dėl galingo euristinės analizės mechanizmo ir kasdien atnaujinamos virusų aprašų bazės turėtų patikimai saugoti kompiuterį nuo visų tipų virusų, pašto kirminų bei vadinamųjų Trojos arklių. „Dr.Web“ programa sėkmingai pasirodo tarptautinio žurnalo „Virus Bulletin“ (http://www.virusbtn.com/) rengiamose antivirusinių programų peržiūrose, yra ne kartą pelniusi „100% Virus Bulletin“ titulą.

Suprantama, antivirusinės programos „Dr.Web“ vertimas dar bus tikslinamas bei tobulinamas, numatoma sulietuvinti ir naujas programos versijas, tad mielai lauksime jūsų atsiliepimų bei pasiūlymų.

ALFA PLIUS OMEGA, 2003, Nr. 1(17)

2003 04 14. 12,5 sp. l. Tiražas 1000 egz. Užs. Nr. 1434
Leidykla TEV, Akademijos g. 4, LT-2021 Vilnius
Spausdino UAB „Mokslo aidai“
A. Goštauto g. 12, LT-2600 Vilnius
Viršelį spausdino UAB „Petro ofsetas“
Žalgirio g. 90, LT-2600 Vilnius