IZBOR ANTIVIRUSNOG SOFTVERA ZA ZAŠTITU RADNIH STANICA

Prof. dr Dragan D. Milanović
Mašinski fakultet u Beogradu

Doc. dr Mirjana Misita
Mašinski fakultet, Beograd

Doc. dr Dragan Lj. Milanović
Mašinski fakultet, Beograd

Dr Danijela Tadić
Mašinski fakultet, Kragujevac

S obzirom na značaj zaštite informacionih sistema u savremenom poslovanju, u okviru ovog primera bavićemo se izborom antivirusnog softvera za zaštitu radnih stanica. Poznato je da nijedan softver ne pruža kompletnu zaštitu, pa je zato zadatak menadžmenta da odabere onaj koji na najbolji mogući način zadovoljava postavljene kriterijume.

Samo jedan deo celokupne zaštite informacionih sistema preduzeća predstavlja zaštita radnih stanica na kojima zaposleni svakodnevno obavljaju svoje radne zadatke. Zaštita radnih stanica podrazumeva instalaciju antivirusnog sistema zaštite.

Zbog toga je pre donošenja odluke o izboru antivirusnog softvera neophodno sprovesti testiranja antivirusnih softverskih rešenja, a menadžment preduzeća može da nakon dobijanja rezultata tih testova lakše donese odgovorajuću odluku primena Sistema za podršku odlučivanju (SPO). U konkretnom slučaju to je softver Criterium Decision Plus 3.0.4/S.

Dobra antivirusna zaštita treba da zadovolji odgovarajuće kriterijume odnosno pokaže dobre rezultate prilikom testiranja. Neophodno je da se često obnavlja baza virusa, što automatski poveća mogućnost detektovanja potencijalnih pretnji. Takođe neophodno je da ima sposobnost da fajlove, na kojima su detektovani virusi ili maliciozni kodovi, dezinfikuje. Poželjno je da antivirusni softver ima mogućnost brzog skeniranja računara, s obzirom da je skeniranje neophodno svakodnevno, a da pritom zauzetost memorije i zagušenje procesora nisu veliki.

U konkretnom slučaju, sagledavanjem rezultata testiranja i detaljne analize rezultata dobijenih primenom navedenog softvera, odlučeno je da se antivirusni softver Nod32 prihvati kao trenutno najbolje rešenje i da se izvrši negova primena u preduzeću.

Ključne reči: *Sistemi za podršku odlučivanju, softver, kriterijum, alternativa.*

CHOOSING ANTIVIRUS SOFTWARE FOR WORKSTATION PROTECTION

According to significance of information systems protection in modern business, this paper describes method of choosing antivirus software for workstations. Although, complete protection cannot be achived using of one of existing antivirus software, managers should choose solution which in given criteria could give adequate support.

Problem of workstation protection represents just one part of informaton system protection policy in an enterprise. Workstation protection implies installation of antivirus protection system. Before making decision of implementation adequate antivirus protection system, it is necessery to perform testing several antivirus package. We use decision support system for multicriteria decision in testing performance of several antivirus protection systems.

CDP is used by public institutions and managers for support in consensus and structuring decision making process in situations where lot of criteria, alternatives and users are involved. It combines power of system analysis, easy of use and good graphic interface. Also, CDP enables decisions analysis and it is very usefull for consultants to explain clients process of judgment in making decision or advice. Designed decision making model for choosing antivirus softvare for workstations protection enables multicriteria optimization of results which are attained by antiviral software testing.

Good antivirus protection system, should satisfy given set of criteria, primarliy. Further, it is necessery to permanently update virus database, which give to it potential for detecting potential threats. Also, it is necessery that choosen antivirus protection system has ability for desinfection detected viruses and threatening codes. Speed of system scanning, memory used, processor slow down are also criteria which we use in evaluation of antivirus protection systems.

In case of testing antivirus softvare for this particular enterprise, results by applying decision support systems indicate that Nod32 represents best solution for implementation.

Key words: Decision support system, software, creteria, alternative..

UVOD

Zaštiti informacionih sistema u preduzeću, neophodno je dati odogovarajući značaj i na taj način sačuvatu podatke od zloupotreba i malicioznih kodova. Trenutno na softverskom tržištu ne postoji softver koji može pružiti kompletnu zaštitu informacionog sistema, pa u takvoj situaciji menadžment ili donosioci odluka o IT segementu u preduzeću, treba da izaberu ono antivirusno rešenje koje na najbolji mogući način zadovoljava postavljene kriterijume.

Zaštita radnih stanica na kojima zaposleni svakodnevno obavljaju svoje radne zadatke, predstavlja samo jedan deo celokupnog sistema IT zaštite preduzeća. Zaštita radnih stanica podrazumeva instalaciju antivirusnog sistema zaštite.

Dobra antivirusna zaštita treba da zadovolji odgovarajuće kriterijume odnosno pokaže dobre rezultate prilikom testiranja. Neophodno je da se često obnavlja baza virusa, što automatski poveća mogućnost detektovanja potencijalnih pretnji. Takođe neophodno je da ima sposobnost da fajlove, na kojima su detektovani virusi ili maliciozni kodovi, dezinfikuje. Poželjno je da antivirusni softver ima mogućnost brzog skeniranja računara, s obzirom da je skeniranje neophodno svakodnevno, a da pritom zauzetost memorije i zagušenje procesora nisu veliki.

Zbog toga je pre donošenja odluke o izboru antivirusnog softvera neophodno sprovesti testiranja antivirusnih rešenja, a menadžment preduzeća nakon dobijanja rezultata tih testova može lakše da donese odgovorajuću odluku, a jedan od načina je i primena Sistema za podršku odlučivanju (SPO). U konkretnom slučaju to je softver *Criterium Decision Plus 3.0.4/S.*

DEFINISANJE PROBLEMA I ULAZNIH VELIČINA

Početkom 90-tih godina dolazi do jačanja globalnog povezivanja i sve veće promene Intrneta i World Wide Web-a. Komunikacija se seli u područje virtuelne stvarnosti, a informacioni sistemi postaju sve više deo tog nerealno sveta. Finansijski i drugi tokovi se odvijaju sve više unutar njega, a razvijeni svet postaje zavistan od računarskih i informacionih sistema. Najčešća tema koju danas povezujemo s Internetom je upravo njegova sigurnost, odnosno bolje rečeno nesigurnost podataka koji svakodnevno kruže među milionima njegovih korisnika. /8/

S obzirom na značaj zaštite informacionih sistema u savremenom poslovanju, u okviru ovog primera bavićemo se izborom antivirusnog softvera za zaštitu radnih stanica. Kako bismo dobili podatke, odnosno kriterijume na osnovu kojih ćemo nastojati da u okviru Sistema za podršku odlučivanju, odaberemo najbolju od alternativa prethodno smo izvršili testiranje antivirusnih rešenja. Testirana su sledeća rešenja:

1. *Norton*
2. *Kaspersky*
3. *PCCillin*
4. *AVG*

Kontakt: Dr Dragan D. Milanović
Mašinski fakultet u Beogradu
Kraljice Marije 16, 11000 Beograd
E-mail: ddmilanovic@mas.bg.ac.yu

5. *Sophos*
6. *NOD32*

METODOLOGIJA TESTIRANJA

Testiranje antivrusnih rešenja izvršeno je sa istim skupovima inficiranih fajlova (1248), testiranje Real time skenera izvrseno je sa istim skupom od 10 inficiranih fajlova, testiranje Mail skenera izvršeno je ubacivanjem zaraženih fajlova u atačment mail-a, dok je testiranje opterećenja procesora i memorije tokom skeniranja izvšeno upotrebom Performance Monitora, tabela 1. Kao relevantni podaci za poređenje su uzimani: broj detektovanih virusa, broj dezinfikovanih fajlova, brzina skeniranja, kao i opterećenost procesora i memorije za vreme skeniranja. Testiran je i Real time skener na File Serveru, kao i Mail skener. Takođe je testirana mogućnost rada antivirusnih rešenja u Safe Mode-u.

Nakon dobijanja rezultata testiranja, pristupićemo analizi dobijenih rezultata korišćenjem programa Criterium DecisionPlus (verzija 3.0.4/S). To je softver koji pruža podršku u procesu odlučivanja izbora najboljeg antivirusnog programa i to na osnovu rangiranja alternativnih rešenja prema postavljenim kriterijuma.

Antivirusni softver **Norton** nudi jednostavnu instalaciju upravljačke konzole i mogućnost udaljene instalacije softvera na klijentskim računarima. Korisnički interfejs je pregledan i lak za snalaženje. Nakon instalacije ne zahteva restartovanje računara.	Upravljačka konzola antivirusnog softvera **Kaspersky** nudi dosta podešavanja, mada je upravljanje njom blago iskomplikovano. Mana ovog softvera je nemogućnost skeniranja fajlova zaštićenih lozinkom. Softver zahteva restart računara nakon instalacije.
PCCillin poseduje dobru upravljačku konzolu koja omogućuje i udaljenu instalaciju, konfiguraciju. Korisnički interfejs je pregledan i jednostavan za upravljanje. Po instalaciji ne zahteva restart.	**AVG** antivirusni softver poseduje upravljačku konzolu koja je jednostavna i pregledna za rukovanje. Omogućena je udaljena instalacija i konfiguracija softvera. Interfejs je moguće izabrati na jednom od 10 jezika, među kojima i srpski.
Antivirusni softver **Sophos** nudi jednostavnu instalaciju, interfejs je pregledan i lak za korišćenje. Takođe omogućava udaljenu instalaciju i konfiguraciju softvera. Nakon instalacije ne zahteva restart.	Antivirusni sofver **Nod32** nudi jednostavan korisnički interfejs, vrlo pregledan i lak za korišćenje. Poseduje odvojena podešavanja za različite *scan engine*-e (AMON, NOD32, IMON, EMON, DMON).

Tabela 1: Testirannje antivirusnog softvera

		NORTON	PC CILLIN	NOD32	AVG	KASPERSKY	SOPHOS
Radna stanica	Brzina skeniranja	173' 26"	8' 47"	31'	25' 27"	78' 14"	15'
	Broj detektovanih virusa	1365	1206	1230	1209	1414	860
	Broj dezinfikovanih fajlova	696	377	1036	394	519	859
	Prosečno zagušenje procesora (%)	46,7	23	31,1	49,3	41,7	32.7
	Real time - Broj detektovanih virusa	4	7	3	5	5	4
File Server	Broj detektovanih virusa	4	7	3	5	2	4
Mail Skener	Outlook Express	4	7	8	8	8	4
	Microsoft Outlook	4	7	8	7	6	4
Safe Mode	Rad u Safe Mode-u	DA	NE	DA	DA	DA	DA

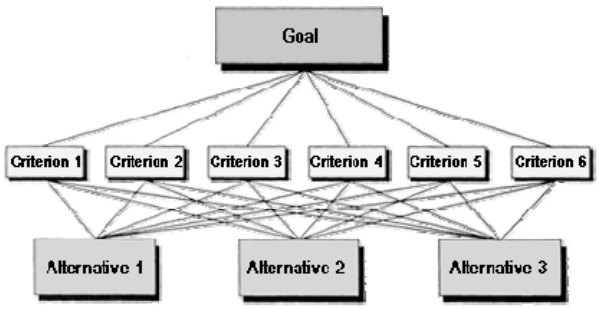
CRITERIUM DECISION PLUS - CDP 3.0

Criterium Decision Plus 3.0 (CDP 3.0) je softver razvijen od strane *Info Harvest*-a. *CDP* pomaže korisnicima u donošenju kompleksnih odluka. Problem višekriterijumskog odlučivanja obično uključuje izbor jedne od brojnih alternativa na osnovu toga koliko su te alternative dobro rangirane u odnosu na izabranu grupu kriterijuma. Sami kriterijumi se vrednuju u smislu važnosti za onoga koji donosi odluku, a ukupan „rezultat" neke od alternativa predstavlja ponderisanu sumu njenog rangiranja prema svakom kriterijumu.

CDP pruža podršku za dve metodologije koje se koriste za višekriterijumske analize. To su:

- *AHP (Analytic Hierarchy Process)*
- *SMART (Simple Multi-Attribute Rating Technique).*

AHP omogućava korisnicima da izvrše procenu odgovarajuće težine višestrukih kriterijuma na intuitivan način, slika 1. Njegova najveća inovacija bila je uvođenje poređenja u parovima. Poređenje u parovima predstavlja metod zasnovan na istraživanju koje pokazuje da, kad kvantitativno rangiranje nije dostupno, ljudi i dalje znaju da prepoznaju da li je neki kriterijum važniji od drugog. Dr. Thomas Saaty, izumitelj AHP metodologije, ustanovio je dosledan način za konvertovanje ovakvih poređenja „u parovima" (X je važnije od Y) u seriju brojeva koji predstavljaju odgovarajući prioritet svakog kriterijuma.



Slika 1. Prikaz AHP tehnike (www.wikipedia.org)

Nedostatak AHP metode može predstavljati „inverzija ranga" („Rank Reversal"). Pošto su mišljenja u AHP po prirodi relativna, promena grupe alternativa može promeniti rezultate odlučivanja kod svih alternativa. Prikazano je da ako se završenom modelu doda čak i mala, vrlo oskudna alternativa, alternative sa najboljim rezultatima ponekad obrnu svoje odgovarajuće rangiranje. Upravo zbog toga, ukoliko postoji velika verovatnoća da će se nove alternative dodavati modelu posle njegove početne izrade, tada bi SMART tehnika predstavljala dobar izbor.

U tehnici prostog višeatributskog rangiranja (***SMART***), rangiranja alternativa se dodeljuju direktno, u prirodnim razmerama kriterijuma (gde je to dostupno). Na primer, kod procene kriterijuma „najveća brzina" za motorna vozila, prirodna skala bila bi u rasponu od 100 do 200 milja na sat. Kako bi se ponderisanje kriterijuma i rangiranje alternativa odvojilo koliko je god moguće, različite skale kriterijuma treba konvertovati u zajedničku internu skalu. U SMART-u ovo izvršava matematički onaj ko donosi odluku pomoću „funkcije vrednosti" („Value Function"). Međutim, da bi se bolje prikazala ljudska psihologija u donošenju odluka, ne korišćenje linearnih funkcija često predstavlja prednost. Primenom ove tehnike promena broja alternativa koje se razmatraju neće promeniti rezultate odlučivanja prvobitnih alternativa, kao što je slučaj kod AHP tehnike.

Do donošenja konačnog rezultata i analize dobijenih rezultata koristeći ovaj softver prolazimo kroz nekoliko faza. Prva faza (tzv. *Brainstorming*) predstavlja generisanje ideja, odnosno povezivanje zadatih kriterijuma. Nakon toga sledi povezivanje unetih kriterijuma sa postojećim alternativama, što predstavlja generisanje hijerarhije. Nakon toga vrši se rangiranje kriterijuma, što predstavlja inpute koje dajemo softveru, a koje on kasnije koristi za odabir najboljeg rešenja odnosno najbolje alternative. Nakon toga program nam pruža pregled i analizu dobijenih rezltata. Na taj način donosioc odluka u preduzeću odlučuje da li će prihvatiti rešenje koje mu je softver ponudio, jer na kraju ipak je menadžment preduzeća taj koji donosi konačnu odluku.

DEFINISANJE CILJA, ALTERNATIVA I KRITERIJUMA – BRAINSTORMING

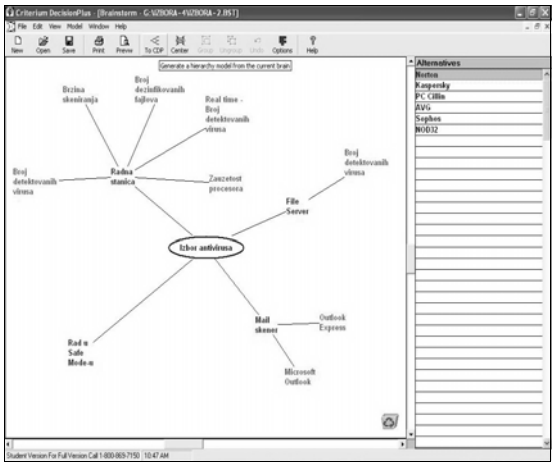
Prilikom otvaranja programa i pokretanja komande *File/New*, dobijamo mogućnost definisanja cilja, alternativa i kriterijuma na osnovu čega ćemo kasnije generisati hijerarhiju. U okviru kružnog polja „*Goal*", koje se automatski pojavljuje na ekranu prilikom otvaranja novog fajla, definišemo naš cilj, u našem slučaju to je „Izbor antivirusa". Sa desne strane programa možemo primetiti polja koja predstavljaju mesta za unošenje alternativa (*Alternatives*). U ta polja unosimo naše alternative. U našem slučaju to su antivirusna rešenja koja smo prethodno

obuhvatili testiranjem (**PCCillin, NOD 32, Kaspersky, Sophos, AVG, Norton**).

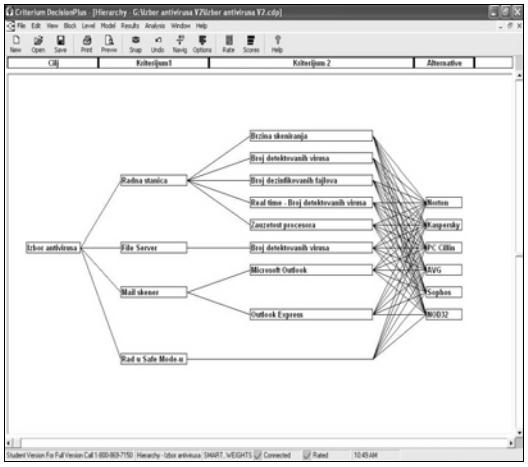
Nakon definisanja cilja i alternativa moramo uneti i kriterijume i podkriterijume koje ćemo kasnije vrednovati i na taj način pružiti mogućnost programu da na osnovu unetih kriterijuma i dodeljenih težinskih ocena izvrši izbor najpovoljnije alternative. Klikom u prazno polje u prostoru oko cilja koji smo već definisali otvara nam se textbox u koji unosimo kriterijume. Nakom unosa svih kriterijuma vršimo njihovo povezivanje sa ciljem tako što textbox prevučemo preko textbox-a sa ciljem. U našem slučaju imamo dve linije kriterijuma:

- *Radna stanica*
  - *Broj detektovanih virusa*
  - *Broj dezinfikovanih fajlova*
  - *Brzina skeniranja*
  - *Prosecno zagušenje procesora (%)*
  - *Real-time protekcija*
- *File Server*
  - *Broj detektovanih virusa*
- *Mail skener*
  - *Microsoft Outlook*
  - *Outlook Express*
- *Rad u SafeMode-u*

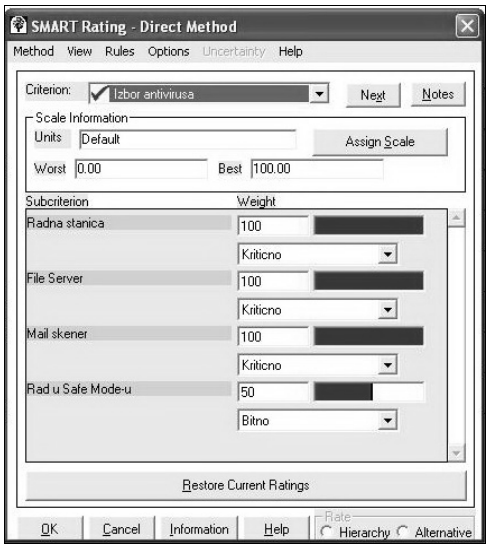
Nakon povezivanja svih kriterijuma i podkriterijuma sledeći korak predstavlja generisanje hijerarhije. Da bismo to učinili potrebno je da u meniju odaberemo opciju *Model*, pa iz padajuće liste odaberemo opciju *Generate Hierarchy* ili klikom na dugme „*To CDP*“ koje se nalazi na Toolbar - u (slika 2). Kada to uradimo dobijamo generisanu hijerarhiju prikazanu na slici 3.



Slika 2. Definisanje cilja, alternativa i kriterijuma



Slika 3. Generisana hijerarhija



Slika 4. Ocenjivanje kriterijuma

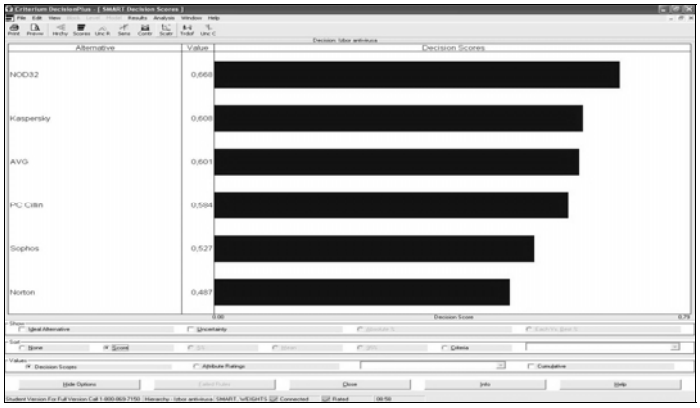
DODELJIVANJE TEŽINSKE OCENE KRITERIJUMIMA

Pre nego što počenomo sa ocenjivanjem neophodno je da prvo odaberemo tehniku ocenjivanja. Na glavnom meniju odabraćemo opciju *Mode*l i odabrati opciju S.M.A.R.T. iz padajuće liste u okviru menija *Tehnique – Alternatives* /9/. Nakon što smo definisali tehniku ocenjivanja pristupamo rangiranju kriterijuma kako bismo odredili koji od postavljanih kriterijuma ima za nas najveću važnost. Da bismo to uradili pozicioniraćemo se na „Izbor antivirusa" i nakon toga kliknuti na dugme *Rate* koje se nalazi na Toolbar-u. Nakon toga pristupamo ocenjivanju kriterijuma, ali prethodno moramo da definišemo numeričku i verbalnu skalu ukoliko ne želimo da koristimo one koje su postavljene kao Default. U našem primeru izvršićemo promenu verbalne skale. Da bismo to uradili kliknućemo na *Assign scale*. Zatim čekiramo opciju *Verbal* i klikom na *New* otvara nam se prozor u okviru koga definišemo novu verbalnu skalu. Kada smo definisali numeričku i verbalnu skalu, pristupamo ocenjivanju kriterijuma slika 4.

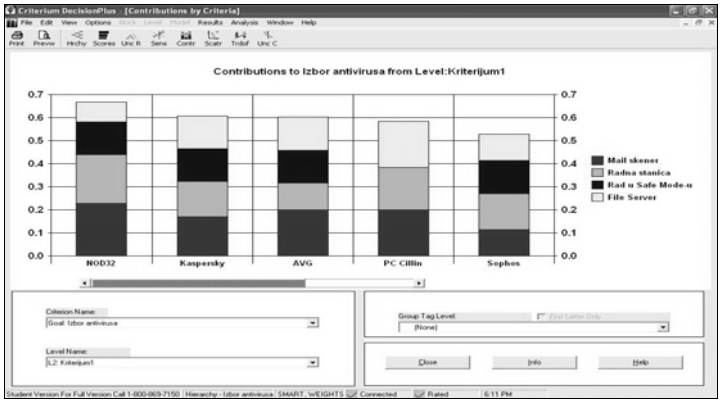
Klikom na dugme *Next*, slika 4, pristupamo sledećem kriterijumu za ocenjivanje. U toku tog postupka u svakom trenutku možemo po želji definisati novu verbalnu ili numeričku skalu. Kada ocenimo sve kriterijume program nas o tome obaveštava. Nakon klika na dugme OK dobijamo kalkulisani rezultat.

Na taj način program nam predstavlja izabranu alternativu koja po njemu, a na osnovu unetih kriterijuma, predstavlja najbolje rešenje. Kao što možemo da primetimo na osnovu unetih kriterijuma program je rangirao antivirusno rešenje *Nod32* kao najbolje rešenje, slika 5. Dalje je na nama da na osnovu analize rezultata odlučimo da li ćemo prihvatiti ono što nam program predlaže ili ne. Ukoliko čekiramo opciju *Criteria* možemo izvršiti prikaz rezultata prema svakom zasebnom kriterijumu.

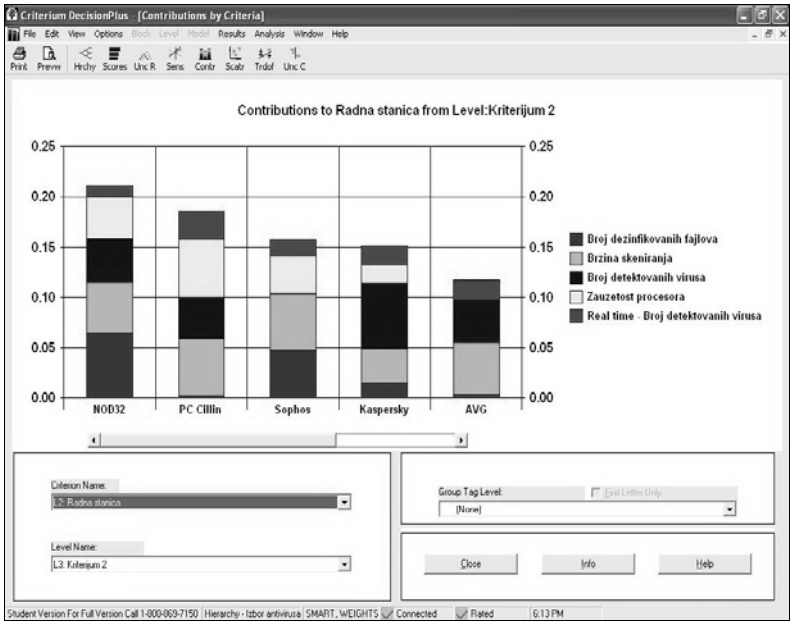
Dosta detaljniji grafički prikaz rezultata dobijamo klikom na dugme *Contr* koje se nalazi na Toolbar-u. Ovakav prikaz nam omogućava jednostrani pregled rezultata po osnovu više kriterijuma, slika 6. Takođe, ukoliko želimo prikaz odrađenog kriterijuma možemo ga prikazati nakon odabira iz opcije *Criterion name,* slika 6.



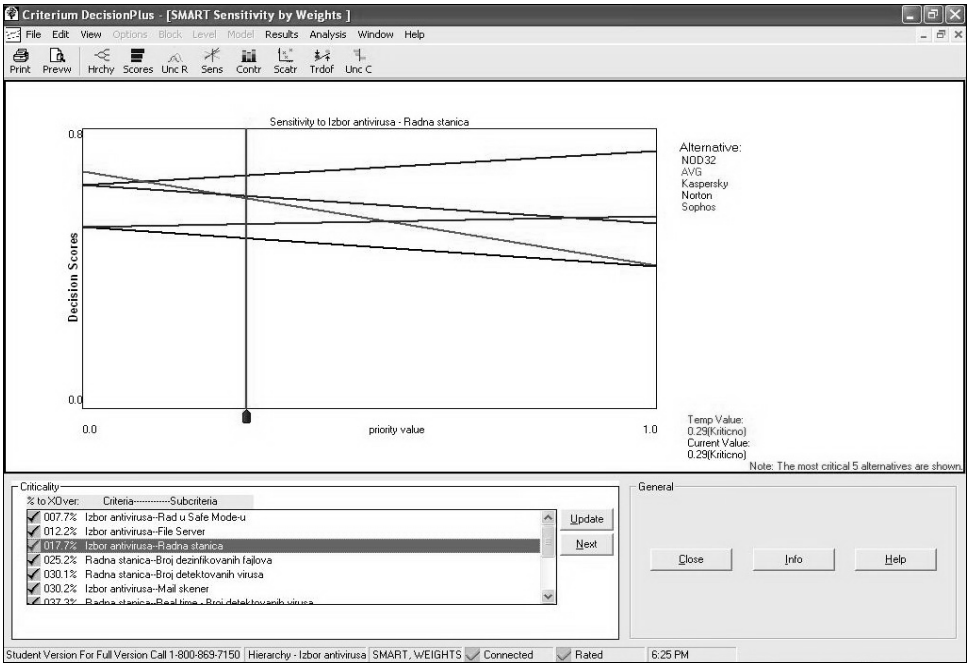
Slika 5. Konačan rezultat



Slika 6. Grafički prikaz – Kriterijum „Izbor antivirusa"



Slika 7. Grafički prikaz – Kriterijum „Radna stanica“



Slika 8. Senzitivna analiza za kriterijum „Radna stanica“

ANALIZA REZULTATA

Izborom opcije *Sens* na toolbar-u vršimo analizu osetljivosti rezultata na definisane težinske ocene kriterijuma.. Kako bismo prikazali rezultate na grafikonu na osnovu kojih ćemo vršiti analizu moramo kliknuti na dugme *Update*. Nakon aktiviranja opcije *Update* dobijamo sledeći prikaz (slika 5). Senzitivna analiza nam pruža kompletan pregled i sagledavanje rezultata, a sa desne strane grafikona vidimo legendu koja prikazuje alternative. Možemo primetiti da je svaka alternativa različite boje. Boja kojom je naziv alternative ispisan odgovara boji linije na grafikonu. Takođe, možemo primetiti i vertikalnu crvenu liniju. Ta linija definiše važnost koju smo dodelili određenom kriterijumu koji je trenutno prikazan. Mesto gde se horizontalne linije seku sa crvenom vertikalnom linijom pruža nam uvid u moguća preklapanja alternativa koje smo razmatrali. Ispod grafikona, u donjem levom uglu ekrana, postoji opcija *Criticality*. Klikom na neki od kriterijuma u tom prozoru prikazuje se grafikon

vezan za izabrani kriterijum. To nam omogućava senzitivnu analizu svakog zasebnog kriterijuma.

Na osnovu dobijenih rezultata i na osnovu senzitivne analize možemo zaključiti da prema postavljenim kriterijumima najbolje antivirusno rešenje koje bismo trebali da primenimo predstavlja rešenje kompanije ESET – *Nod32*.

ZAKLJUČAK

Nakon izvršene analize rezultata dobijenih testiranjem antivirusnih rešenja uz pomoć ovog softvera možemo zaključiti da nam je softver pomogao pri donošenju konačne odluke. Dobar korisnički interfejs ovog softvera i lako upravljanje njime u znatnoj meri olakšava proces donošenja menadžerskih odluka. Program nam pruža mogućnost da, ukoliko želimo da izvršimo neke izmene vezane npr. za definisanje kriterijuma ili dodeljivanje težinske ocene kriterijumima, to možemo uraditi u svakom trenutku. Softver automatski generiše sve promene.

Ukoliko ipak želimo samo da promenimo stepen važnosti određenog kriterijuma to možemo izvršiti i prilikom senzitivne analize rezultata i to direktno sa grafikona. Na grafikonu se nalazi vertikalna crvena linija koja ima klizač na kraju i njegovim pomeranjem direktno menjamo relativnu važnost posmatranog kriterijuma u odnosu na ostale kriterijume. Na taj način može doći i do promene konačnog rezultata analize.

U konkretnom slučaju, sagledavanjem rezultata testiranja i detaljne analize rezultata dobijenih primenom navedenog softvera, odlučeno je da se antivirusni softver ***Nod32*** prihvati kao trenutno najbolje rešenje i da se izvrši negova primena u preduzeću.

LITERATURA

/1/ Milanović, D.D., Tadić, D., Misita, M.,*Informacioni sistemi menadžmenta sa primerima*, Megatrend univerzitet primenjenih nauka, Beograd, 2005.

/2/ http://dssresources.com/history/dsshistory.hml

/3/ http://polj.ns.ac.yu/english/people/download/sas_5.pdf

/4/ http://www.cqm.co.yu

/5/ http://www.cet.co.yu/cetcitaliste/CitalisteTekstovi/SPO1.pdf

/6/ http://www.infoharvest.com

/7/ http://www.wikipedia.org

/8/ Aleksić-Marić V., Stojanović D., Rješavanja sigurnosnih rizika u elektronskom poslovanju i informaciona ekonomija, Časopis Istraživanja i projektovanja za privredu, 16/2007, str. 53-62, Beograd,

/9/ Milanović, D.D., Ranđić D., Ristić Lj.,Izbor menadžera održavanja primenom sistema za podršku odlučivanju, Časopis Istraživanja i projektovanja za privredu, 18/2007, str. 7-13, Beograd.