

ORGANIZACIONI MODEL IMPLEMENTACIJE BEZBEDNOSNE POLITIKE U OBRAZOVNIM USTANOVAMA

mr Zoran Milanović, dipl. maš. inž.
nastavnik praktične nastave u Višoj železničkoj školi u Beogradu

Apstrakt: *Originalni organizacioni pristup preventivnoj zaštiti računarskih sistema, primenom modela „bezbednosne politike“, garantuju poboljšanje bezbednosti informacija i drugih informatičkih resursa u školi.*

U radu su definisani praktični organizacioni koraci za uvođenje i unapređenje, upravljanja i kontrolu programa zaštite računarskog sistema u školi.

Ključne reči: *Organizacija, informacija, računarski sistem, bezbednosna politika.*

Abstract: *Original organizational approach to preventive protection of computer systems by using "Security policy", guarantees the security of information and other information resource improvement at school.*

Practical organizational steps for implementation and improvement, management and control of the protection program for computer system at school are defined in the paper.

Key words: *Organization, information, computer system, security policy.*

Bezbednost računarskih sistema vrlo često je zanemarena, sprovodi se sporadično „ad-hoc“, bez plana za zaštitu i održavanje, sa velikim finansijskim troškovima zbog neefikasnog korišćenja sopstvenih informacionih resursa. Najčešće se nude polovična rešenja koja se odnose na bezbednost nekog pojedinog istaknutog aspekta u sistemu, dok se drugi elementi zanemaruju. Izvesno je, međutim, da je bezbednost celokupnog sistema uvek proporcionalna bezbednosti najslabije tačke.

Upravljanje bezbednošću računarskog sistema podrazumeva identifikaciju (informacionih) resursa, njihovo vrednovanje, procenu rizika obzirom na moguće pretnje, izradu odgovarajuće bezbednosne politike i njenu implementaciju u stvarnom okruženju i kontinuiranu kontrolu celokupne bezbednosti sa spoljnim i unutrašnjim revizorima.

Odlike dobrog bezbednosnog računarskog sistema su:

1. pravovremeno pružanje relevantnih informacija poslovnom procesu,
2. optimalan način rada, pouzdan, efikasan i efikasan,
3. čuvanje poverljivosti informacija, njihov integritet i celovitost,
4. raspoloživost informacija ili servisa,
5. usklađenost informacija s propisima ili zakonima garancija o njihovoj tačnosti i primerenosti.

Bez odgovarajuće definicije uloga u sistemu nije moguće uspostaviti odgovarajući sistem odgovornosti, a samim time ni zaštite. To se odnosi na identifikaciju resursa, kao i na implementaciju bezbednosne politike.

Prvi uslov za uspešno upravljanje bezbednošću računarskog sistema podrazumeva identifikaciju resursa koji su deo tog sistema. Bez precizne identifikacije resursa nije moguće implementirati njihovu kvalitetnu zaštitu.

Kroz proces identifikacije resursa potrebno je pobrojati sve resurse (prema ISO 17799:2005) unutar računarskog sistema i proceniti njihovu relativnu vrednost za obrazovnu ustanovu. Na temelju toga je moguće kasnije, u procesu upravljanja rizikom, odnosno prilikom analize rizika, efikasno oceniti potreban nivo zaštite za svaki pojedini resurs unutar sistema. [1]

Kvalitetnom identifikacijom resursa nužno je postići sledeće zahteve:

1. identifikovati sve resurse unutar računarskog sistema,
2. proceniti vrednost resursa,
3. ustanoviti vlasnika, odnosno osobu koja je odgovorna za resurs,
4. ustanoviti njegovo fizičko ili logičko mesto u sistemu i
5. napraviti odgovarajuću dokumentaciju.

I na kraju, u saradnji informatičkog osoblja i pravne službe izraditi normativni akt - Pravilnik o zaštiti, koji će definisati bezbednosnu politiku zaštite računarskog sistema. Iz tog pravilnika će proizaći i nužnost donošenja niza drugih akata, standarda i sprovođenja niza aktivnosti kojima će se detaljno i operativno rešiti, i regulisati zaštita računarskog sistema.

Na temelju proučavanja i analize postojećih normativnih akata, standarda, procesa, organizacije i tehnologije rada računarskog sistema i uvažavajući važeće međunarodne standarde (UN, EU, ISO 17799), treba doneti Pravilnik o zaštiti koji će sadržati:

- predmet normativne regulative (šta je obuhvaćeno merama i aktivnostima koje se propisuju),
- definicije pojmova i izraza koji se koriste,
- ko je odgovoran za zaštitu,
- šta je predmet zaštite,
- koji su izvori ugrožavanja računarskog sistema,
- propisati mere i aktivnosti zaštite (najveći deo u Pravilniku o zaštiti), propisati kontrolu funkcionisanja sistema zaštite u računarskom sistemu, itd.

Najveći otpor uvođenju ovih mera predstavlja birokratija, koja u želji da sačuva postojeći sistem funkcionisanja i sebe samu od redukovanja i gubitka značaja,

permanentno upozorava na sukob nadležnosti, kao i zakonske regulative koje su u ovoj oblasti tek u povoju.

Da bi se prenebregli svi postojeći, kao i budući problemi koje je nemoguće predvideti, potrebno je praviti sistem nezavisno od tehnologije. Naime, ne sme se koristiti postojeća tehnologija kao osnov za izgradnju sistema bezbednosti, već je potrebno postaviti pravila koja će omogućiti funkcionisanje nezavisno od raspoložive tehnologije, čime bi se eliminisao problem predviđanja razvoja kao i kompatibilnost postojećih i budućih tehnologija. Sledeća stvar o kojoj se mora voditi računa je funkcionalnost, a ne modernizacija po svaku cenu. Ne treba srljati u nabavku najnovijih tehnoloških rešenja, već voditi računa o tome da sistem funkcioniše i da noviteti olakšavaju, a ne otežavaju proces zaštite.

Problem računarske bezbednosti daleko je veći od tehničkih rešenja ili proizvoda. Računarska bezbednost je proces koji obuhvata različite aspekte rada i korišćenja računarskih sistema, a pre svega je postupak definisanja odgovornosti za sve učesnike u korišćenju računarskih sistema.

Danas u našim obrazovnim ustanovama malo je računarskih sistema zaštićeno prema preporukama struke ili propisanih standarda, naročito ako prihvatimo definiciju računarske bezbednosti kao procesa, a ne skupa tehničkih mera. Za standarde se može reći da oni pokrivaju tehničke detalje i primenjenu tehnologiju, dok procesi se baziraju na standardima i u njima je predstavljen konkretan postupak neophodnih aktivnosti. Cilj razdvajanja je da se standardi i procesi mogu menjati bez promene bezbednosne politike.

Poštovanje bezbednosnih standarda nije garancija potpune zaštite računarskog sistema, već minimum koji mora da bude ispunjen da bi računare u mrežnom okruženje uopšte imalo smisla koristiti. U tom smislu svaki realan sistem zaštite zahteva kontinuiranu nadogradnju i usavršavanje, bez obzira na do tada ostvareni kvalitet. Korektivne akcije treba usmeriti na modifikaciju rešenja sa uočenim slabostima u prihvatljiva i zadovoljavajuća rešenja, ili, u nemogućnosti modifikacije, njihovu eliminaciju iz sistema, kao i iznalaženje, razvijanje i primenu sopstvenih originalnih rešenja na planu zaštite.

Mere organizacionog karaktera spadaju u kategoriju netehničkih mera, i kao takve ne degradiraju rad sistema, već naprotiv, znatno doprinose povećanju njegove raspoloživosti i produktivnosti. Od ovih mera treba početi, maksimalno ih iskoristiti i sa njima prekriti ceo informacioni sistem. Isto tako, ove mere, kao samostalan i delotvoran instrument, predstavljaju najjeftinije i najefikasnije sredstvo u pravcu preventivnog odvrćanja od nedozvoljenih aktivnosti, kao i u sprečavanju i otkrivanju brojnih nedozvoljenih ponašanja i delovanja. [3]

Bezbednosna politika

Cilj bezbednosne politike (politike računarske zaštite) je da daje opšta pravila sa kojima moraju biti upoznati svi zaposleni. Bezbednosna politika je skup pravila i postupaka koji regulišu kako organizacija upravlja, štiti i distribuira informatičke resurse. Osnovna korist koju organizacije vide od uvođenja bezbednosne politike je izbegavanje rizika uzrokovanih ljudskim faktorom. Takvi rizici mogu biti veći od onih koje izaziva konkretna tehnologija. Politika mora biti predstavljena u formi koja je relevantna, dostupna i razumljiva čitaocu kome je namenjena. Na generalnu bezbednosnu politiku, za koju je preporučeno da bude što kraća, nadovezuju se politike zaštite određenih aspekata informacionih tehnologija — elektronske pošte, interneta, fizičke zaštite, antivirusnoj zaštiti, zaštiti od spama, zaštiti od špijunskih i drugih malicioznih programa, korišćenja lozinki, itd. Sve ove politike treba da budu lišene tehničkih detalja i pisane tako da se menjaju samo ako dođe do promene filozofije poslovanja.

Danas se posebna pažnja posvećuje zaštiti informacija i znanju kao najvažnijim resursima za organizaciju, instituciju ili pojedinca. Bezbednost informacija i informacionih procesa postaje prioritetna za očuvanje poslovnih i svih drugih društvenih procesa.

Metodologija sprovođenja zaštite računarskih sistema temelji se na međunarodnoj normi ISO 17799, kojom se definiše okvir za upravljanje i organizovanje informacione bezbednosti, ali i na drugim važećim normama, standardima i profesionalnim preporukama specijalizovanih organizacija za informacionu bezbednost.

Dobro planiranje i organizovanje programa zaštite računarskih sistema obuhvata izradu bezbednosne politike, analizu bezbednosnih rizika za pojedina područja, planiranje i sprovođenje bezbednosnih mera relevantnih za upravljanje radom računarskog sistema i izradu plana sprovođenja operativnih mera bezbednosti.

U Srbiji se, uglavnom, informacije ne smatraju resursom od posebne vrednosti, ne smatraju se imovinom, a ponajmanje kapitalom. Uz takav stav samih vlasnika ili menadžmenta ne čudi da računarska bezbednost zavisi isključivo od iskustva i znanja informatičara. Računarska bezbednost mora krenuti od vlasnika ili menadžmenta. Ovaj proces započinje sasvim jednostavnim korakom, koji i ne zahteva poseban budžet, a to je izrada bezbednosne politike, zapravo pravilnika koji opisuje strategiju sprovođenja programa računarske bezbednosti. Vlasnici ili menadžment u njihovo ime moraju jasno izraziti koje informacije smatraju vrednim, ko je odgovoran za kreiranje i verodostojnost informacija, ko je odgovoran za ispravan rad sistema u celini, šta smeju i šta ne smeju korisnici, kakav nivo usluga očekuju od svojih informatičara, koje obaveze preuzima organizacija prema trećim stranama, na koji način štite privatnost, ...

Dakle, izrada bezbednosne politike računarskih sistema prvi je konkretan i veoma delotvoran korak, koji rukovodstvo neke obrazovne ustanove treba sprovesti u svojoj kući. Time će biti napisan „kućni red“, ali ako se celom poslu pristupi na kompetentan način i uz podršku svih njenih učesnika, onda učinak može biti i mnogo veći.

Ne postoji standardna forma ili obrazac po kojem se oblikuje bezbednosna politika. Po pravilu se preporučuje da bezbednosna politika ne zadiru previše u tehničke detalje. Dobro napravljena bezbednosna politika postaće verodostojna norma ponašanja u radu s računarskim sistemima i delotvorna podloga za sledeće korake, a to su konkretne organizacijske i tehničke mere kojima se implementiraju ciljevi definisani bezbednosnom politikom. Odgovornost za implementaciju mera snosi menadžment, rukovodioci pojedinih organizacijskih celina, šefovi informatičkih službi, šefovi kadrovskih službi, šefovi službe fizičke zaštite. Stoga bezbednosna politika, osim što treba biti sveobuhvatna tako da svako vidi svoje zadatke, mora jasno definisati šta je to odgovornost u procesu zaštite računarskih sistema.

Prema uobičajenoj praksi u našoj okolini, uglavnom se informatičari smatraju odgovornima za bezbednost računarskog sistema u celini, pa tako i za poverljivost, integritet i raspoloživost poslovnih podataka. Bezbednosna politika, a zatim i praksa koja proizilazi iz politike, informatičare proglašava čuvarima podataka i računarskih sistema i davaocima informacionih usluga. Pravi vlasnici podataka, su dakle osobe odgovorne za njihovu istinitost i verodostojnost, organizatori poslovnih celina gde nastaju takvi podaci. Samo takve osobe mogu reći koliko za njih vredi neki podatak, šta je tajna, a šta stroga poslovna tajna, postoje li zakonske posledice, ako se neki podatak otkrije. Samo su vlasnici podataka merodavni da izreknu ocenu o tome koliko bezbednost i koliko zaštitu žele nad podacima za koje su odgovorni.

Informatičari, koji ponekad bezbednosnu politiku drže previše formalnom i suvoparnom, prvi će pozdraviti ovakav pristup. U nedostatku precizno definisanih nadležnosti i odgovornosti, najčešće informatičari padaju kao prve žrtve kada se pojavi neki bezbednosti incident. No, ako su nadležnosti jasno određene, informatičari će ispuniti svoje obaveze, osim u slučajevima preuzimanja nekih obaveza za koje nemaju dovoljno jaka ovlašćenja ili za koje ne postoji budžet.

Za razvoj i implementaciju same politike bezbednosti zaduženi su ne samo informatičari i rukovodstvo već i svi zaposleni u organizaciji, čak i oni koji u svom dnevnom radu ne koriste računarske sisteme.

Bezbednosna politika mora jasno i nedvosmisleno ukazivati ko je odgovoran za bezbednost. U pojednostavljenom smislu značenja „svi“ su odgovorni znači i „niko“. Korisnici zapravo imaju u sebi prisutna oba elementa da su primarno zaduženi za bezbednost sistema, i da u isto vreme predstavljaju najveću opasnost i izazov za bezbednost. Bezbednosna politika mora zahtevati od svih korisnika da potpišu ugovor, koji jasno određuje njihovu specifičnu bezbednosnu odgovornost i potrebno znanje koje bi trebalo da u sebi sadrži elemente poznavanja sistema i podataka.

Svi zaposleni moraju da se ponašaju u skladu sa bezbednosnom politikom i organizacija mora da prepozna ovu činjenicu. Zbog toga je neophodno da sve politike budu pisane jezikom koji koriste zaposleni.

Menadžment organizacije sve više shvata i prepoznaje važnost bezbednosne politike, ne samo na informatičkom nivou, već i na nivou upravljanja organizacijom. Postojanje bezbednosne politike je prva i osnovna mera koja se očekuje od neke organizacije. Bezbednosna politika mora nužno biti podržana konkretnim bezbednosnim merama, procedurama i redovnim kontrolama. Rukovodstvo i vlasnici propisuju zbog čega se računarski sistemi trebaju štititi, i mnogo važnije, ko je odgovoran za to. Ovo je, dakle, važna mera, koja se može pokrenuti s relativno malo troškova, a njeni efekti biće dalekosežni.

Direktor ili predsednik kompanije i upravni odbor moraju odobriti politiku i obezbediti resurse – ljudske i finansijske – da bi bezbednost postala realnost.

Mora se shvatiti kako bezbednost računarskog sistema nije jednokratna akcija niti se može redukovati na određeni proizvod, koji je nabavljen i opisan kao neophodan ili čak spasonosan. To je skup procesa koji moraju biti tačno definisani, a svaki učesnik dobro edukovan za njihovo sprovođenje.

Sledeći važan zadatak, pre nego što se pređe na mere kojima se operativno sprovode zaključci rukovodstva, je upoznavanje vrednosti informacione imovine za koju se garantuje. Posebno važan stav na samom početku je da se shvati kako informacionu imovinu ne čine samo računari, serveri ili komunikacijska oprema, već i podaci smešteni na diskovima ili oni koji kruže mrežom. To je naravno i najveća prepreka, jer malo je korisnika koji mogu odrediti vrednost svoje informacione imovine. Isto tako malo je članova rukovodstva organizacije koji mogu proceniti kakve će finansijske tragove u troškovima ostaviti kvar računarskog sistema u trajanju od pet minuta ili pet sati. Koliko to znači izgubljenih kupaca? Kolika je šteta nanesena reputaciji banke, ako se otkriju podaci o klijentima? Koliko će klijenata česti „*denial of service*“ napadi oterati drugim *on line* poslovnim sistemima? Kad bi se mogle tačno proceniti štete nastale usled ovakvih nimalo hipotetičkih primera, i program bezbednosti bi bio brže i lakše sproveden.

Temelj i osnovno pravilo kod određivanja mera potrebnih za efikasnu zaštitu podataka je: TROŠKOVI PRIMENJENIH MERA MORAJU BITI MANJI OD POTENCIJALNIH NASTALIH ŠTETA U SLUČAJU DA SE NAPADI ZAISTA I OSTVARE. Skromno stanje naše računarske bezbednosti uzrokovano je upravo nepoznavanjem ključne strane ove nepoznanice: koliko vrede naši podaci?

Na diskovima računara skriva se puno više informacija nego što su toga i svesni njihovi korisnici. To je razlog više za upoznavanje metodologija upravljanja bezbednosnim rizicima. Prema istraživanjima koje je pre nekoliko godina u Sjedinjenim Državama sproveo *Brooking Institute*, čak 85 % vrednosti velikih korporacija leži u nematerijalnoj imovini – svim oblicima informacija, reputaciji, tržišnom poverenju, lojalnosti kupaca... Takva se imovina može urušiti u kratkom roku, ponekad zbog podcenjenog rizika i loše implementiranog informacionog sistema.

Upravljanje nematerijalnom informacionom imovinom podrazumeva puno više umeće i zalaganje rukovodstva, nego što je provera proračuna ili vremenskih okvira izvođenja projekata, kako se najčešće informatika kontroliše.

To uključuje skup novih aktivnosti rukovodstva, usmerenih na poboljšanje njihovog vladanja informacionim tehnologijama.

Bezbednosna politika definiše značaj informacije za organizaciju i posvećenost menadžmenta u zaštiti informacije. To je osnovni dokument visokog stepena važnosti i svi zaposleni moraju da se pridržavaju navedenih mera, a informatičko osoblje će napismeno biti zaduženo bezbednosnom odgovornošću.

Ljudi su uglavnom najosetljivije mesto u svakoj bezbednosnoj šemi. Faktor čovek može da poništi i najbolju zaštitu: zlonameran radnik, nepažljiv radnik, radnik koji nije svestan politike i važnosti informacija u organizaciji.

Za projektovanje sistema zaštite potrebno je odrediti:

- Lice odgovorno za projekat
- Metode identifikacije korisnika i terminala
- Strukture šema ovlašćenja
- Načine detekcije nedozvoljenih pristupa
- Načine integrisanja zaštite u sistemske programe
- Postupke oporavka zbog oštećenja datoteka i rešavanju bezbednosnih incidenata
- Postupke oporavka zbog otkaza sistema,
- Metode izrade rezervnih kopija podataka, nadzora i da li treba koristiti kriptografiju ili ne,
- Kontrole koje treba ugraditi u korišćenje statističkih datoteka,
- Kontrole koje treba ugraditi u operacije pregledanja datoteka.

Još neke prednosti bezbednosne politike su: velike uštede u vremenu i novcu u svim procesima koji se odvijaju unutar jedne organizacije. Elektronski organizovane datoteke dovode do jeftinije obrade, ali i bržeg prikupljanja i pružanja informacija, poboljšanje komunikacije sa korisnicima, kao i do poboljšane razmene informacija kako unutar sistema, tako i sa okruženjem.

Svako odlaganje njegove implementacije će voditi korak nazad u ekonomskom razvoju. Sadašnje, možemo ih nazvati tradicionalističke, garniture menadžmenta se veoma sporo adaptiraju na tehnološku i informacionu revoluciju i skloni su da je tretiraju kao jedan od izazova sa kojima su suočeni i sa kojima tek treba da se pozabave, ne shvatajući da bespotrebno gube vreme i novac, i da je neminovnost bezbednosne politike izvesnija nego ikada.

Za razliku od birokratije, tehnologija evoluirala veoma brzo, tako da donete odluke zahtevaju sprovođenje, a svako kašnjenje prouzrokuje velike finansijske gubitke. Nabavka opreme bez određenog cilja je praktično bacanje para, pošto na godišnjem nivou dolazi do kompletnih promena tehnologija, tako da je ta trka unapred izgubljena. Bez postavljanja sistema, troškovi modernizacije idu do neslučenih visina, a očekivanja korisnika bivaju izneverena.

Sve dok se ovi neophodni koraci ne preduzmu, bezbednosna politika će ostati samo kozmetička promena u sistemu organizacije menadžmenta i koristiće kao izgovor za utrošena sredstva.

Bezbednosne politike u poslovnom svetu izuzetno su restriktivne. Pojednostavljeno rečeno, sve je zabranjeno, osim onog što je izričito dopušteno. A dopušteno je samo ono što je neophodno za obavljanje posla. Akademska zajednica pripada otvorenoj kulturi, okrenuta je komuniciranju, istraživanju, samorazvoju i učenju. Škola brani svoju slobodu i nezavisnost, ne trpi restrikcije. Stoga će ovde i bezbednosna politika biti liberalnija. Težište sprovođenja bezbednosne politike treba biti okrenuto ka obrazovanju, a ne na sužavanju izbora i sankcionisanju. Ipak, u pojedinim delovima bezbednosna pravila će biti jednako restriktivna, kao i ona u komercijalnom okruženju. Postupanje s poverljivim informacijama podleže jednakim pravilima u banci i u školi, a akademska sloboda nikoga ne stavlja iznad zakona, morala i pravila pristojnog ponašanja.

Bezbednosna politika prolazi kroz cikličan postupak predstavljanja, odobravanja, implementacije i održavanja.

Praktičan primer bezbednosne politike u obrazovnim ustanovama

Praktičan predlog konkretnih bezbednosnih mera bio bi:

1. Škola je vlasnik računarskog sistema (hardvera, softvera, računarske mreže i svih podataka).
2. Škola je vlasnik svih procesa i elektronskih transakcija koje se obavljaju u intranet mreži.
3. Korisnici računarskog sistema su dužni da se brinu o celokupnoj informatičkoj imovini (računarskoj mreži, hardveru, softveru i podacima) i da u slučaju uočenih nepravilnosti (oštećenja, smetnji i nedostataka) pismeno obaveste nadležno lice - direktora škole. Ovaj izveštaj mora da sadrži: datum, vreme, detaljan opis uočenog problema i potpis.
4. Pristup i zadržavanje u računarskim kabinetima, laboratorijama i drugim nastavnim entitetima u kojima se nalazi informatička imovina nije dozvoljen trećim licima bez njihove prethodne najave nadležnom licu.
5. Sve računarske kabinete koristiti namenski i prema unapred utvrđenom rasporedu. Promene prostorija bez prethodne najave nisu dozvoljene, kao ni prekoračenje broja prisutnih studenata u odnosu na kapacitete za sedenje. Takođe, nije dozvoljeno ni prenošenje školskog inventara i druge opreme iz prostorije u prostoriju.
6. Za ulazak i boravak studenata u računarskim kabinetima neophodno je prisustvo nastavnika ili nekog od zvanično zaduženih lica.
7. U cilju potpunog nadzora i nesmetanog funkcionisanja računarskih kabineta, obezbediti potpunu i besprekornu funkcionalnost sistema video nadzora, alarmnih uređaja, protivpožarnog sistema, uređaja za kontrolu pristupa, uređaja za neprekidno napajanje (*UPS*) i uređaja za klimatizaciju. Rukovanje ovim uređajima i njihovu funkcionalnu kontrolu obavljati prema uputstvima i preporukama proizvođača. Održavanje vrši isporučilac opreme, odnosno nezavisna specijalizovana firma iz te oblasti, koja u okviru ovih aktivnosti podnosi pismeni izveštaj sa svim neophodnim elementima.
8. Stepen zaštite i održavanja podići na najviši mogući nivo uz korišćenje svih preporuka proizvođača, kao i svih raspoloživih sredstava a sve u cilju nesmetanog korišćenja informatičke imovine i produžavanja njene sposobnosti i gotovosti. Posebne mere zaštite i održavanja sprovesti u najosetljivijim službama (studentska, finansijska i pravno-administrativna);
9. Korisnik se slaže da će pravilno i adekvatno koristiti računarsku imovinu. To znači da nije dozvoljeno: pomeranje, prenošenje, zamena, podešavanje i otvaranje računara i dodatne računarske opreme; nekontrolisano korišćenje mrežnih i drugih štampača, kao i druge mrežne opreme; preinstalacija i podešavanje postojećeg softvera, kao ni instalacija novog, a naročito nelicenciranog softvera (*Corel Draw, Corel Ventura, Adobe Photoshop* itd.); skladištenje fajlova (filmova, muzike, slika itd.) na serveru ili radnim stanicama; korišćenje tuđih naloga i lažno predstavljanje; korišćenje i uništavanje tuđih podataka; napadanje i nanošenje štete drugim računarima u lokalnoj i Internet mreži; nedolično ponašanje na Internetu i slanje kompromitujućih *e-mail* poruka, kao i poruka koje predstavljaju neželjenu poštu – *spam*; prijavljivanje na forumima, *chat* grupama i drugim Internet servisima, kao i ostavljanje adrese škole. Download-ovanje velike količine podataka sa Interneta (muzika, filmovi, slike itd.)
10. Korisnik se slaže da nije i da neće učiniti neautorizovane kopije podataka i softvera.

11. Korisnik se slaže da izabere bezbednosnu šifru (*password*) na promišljen način i da će je držati i očuvati tajnom.
12. Korisnik se slaže da pristupi sistemu i podacima samo na autorizovan način.
13. Profesori i saradnici koji koriste informatičke kabinete su dužni da pre početka časa i praktičnog dela ispita provere svu računarsku opremu na kojoj rade: ispravnost računara i pratećeg softvera.
14. Internet komunikacija se obavlja samo preko Internet servera škole. Pojedinačan modemski pristup Internetu preko telefonske linije nije dozvoljen.
15. Za nesmetano funkcionisanje računarskog sistema odgovorni su svi informatički radnici u okviru svojih ovlašćenja i znanja. Administrator sistema je zadužen za računarsku mrežu, održavanje i zaštitu računarske imovine a posebno za zaštitu i arhiviranje podataka. Saradnik za informatiku, pored direkne pomoći administratoru vrši i nabavku novog hardvera i softvera, njihovo održavanje i zaštitu, kao i prijem i rešavanje reklamacija i tekućih problema. U slučaju da neko od zaduženih osoba ne izvodi precizno planirane aktivnosti i pri tome direktno utiče na celokupnu funkcionalnost informatičke imovine, neophodno je pismeno obavestiti nadležno lice;
16. Pravljenje rezervnih kopija (*backup* podataka) vrši se jednom mesečno i to poslednjeg radnog dana u mesecu, a po završetku radnog vremena i uz prisustvo korisnika ili odgovornog informatičkog lica. Proveru izvršenog posla obavlja kordinator za računarsku tehniku. Pravljenje rezervnih kopija obavljati u računovodstvu, studentskoj i pravno-administrativnoj službi, kao i po pojedinačnim zahtevima drugih korisnika računarskog sistema.
17. Redovna obuka informatičkih kadrova pohađanjem specijalizovanih kurseva, a sa ciljem upoznavanja novih vidova održavanja i zaštite celokupne informatičke imovine;
18. Strogo je zabranjeno unositi i koristiti hranu i piće u svim informatičkim prostorijama.
19. Svi zaposleni i studenti treba da su pristojno i adekvatno obučeni.
20. Sve službe ili pojedinci koji se ne pridržavaju ovih odredbi biće sankcionisani na adekvatan način a prema važećem Statutu škole i postojećim zakonima;
21. Pridržavanje bezbednosne politike mora biti deo svakog obaveznog periodičnog pregleda rezultata rada svakog zaposlenog.
22. Svest o važnosti, tačnosti i ažurnosti podataka treba da bude temelj celog sistema.
23. Svi zaposleni treba da potpišu Izjavu o čuvanju povjerljivih informacija.
24. Politika bezbednosti mora biti objavljena i učinjena dostupnom svim korisnicima.

Pored bezbednosne politike javlja se potreba i za njenim proširenjem pratećim dokumentima, u kojima se definišu pravila za pojedina područja rada. Prateći dokumenti su razni pravilnici. Pisani su kao uputstva za rešavanje konkretnih problema i mogu se češće menjati.

Konačno, idealno i univerzalno rešenje u ovoj oblasti je neizvodljivo i nemoguće je napraviti bezbednosne mere koje će svima odgovarati, jer su različiti i računarski sistemi i budžeti u orgaizacijama. Ipak, predložene mere iz ovog rada bi se sa više od 90% mogle primeniti u bilo kojoj obrazovnoj ustanovi na osnovu sprovedenih analiza i njenih anketiranih korisnika. [2]

LITERATURA

1. ISO/IEC 17799:2005 „Information technology – Security techniques – Code of practice for information security management“

2. Milanović Zoran, ORGANIZACIJA ZAŠTITE RAČUNARSKIH SISTEMA, magistarski rad, Mašinski fakultet Beograd, 2006. godina
3. Petrović R. Slobodan, Kompjuterski kriminal, Ministarstvo unutrašnjih poslova Republike Srbije – Beograd, 2001.