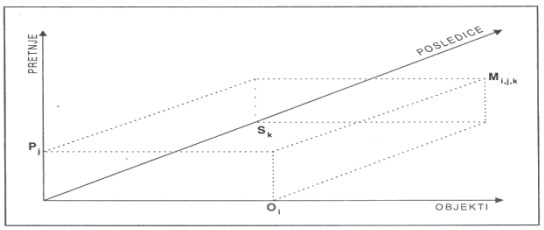
GLAVNI ENTITETI PROBLEMA ZAŠTITE

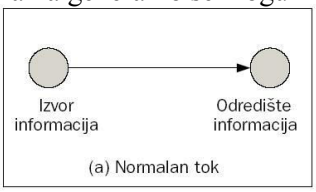
Glavni entiteti problema zaštite u oblasti informacionih sistema su **objekti**, **pretnje**, **posledice**, **mere** i **politika zaštite**. Ovakav pristup omogućava da se problem zaštite, radi jasnoće i lakšeg uočavanja postojećih međuzavisnosti, prikaže i u vidu trodimenzionalne matrice (slika 2) pri čemu svaki element matrice $M_{i,j,k}$ predstavlja skup mera koje bi trebalo primeniti da bi se sprečila posledica S_k, koja može nastupiti ako pretnja P_j ugrozi objekt O_i, tj. $M_z = M(O_i, P_j, S_k)$ [2].



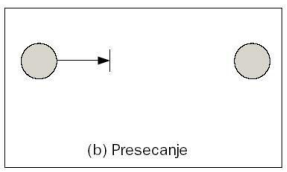
Slika 2. Trodimenzionalna matrica mera zaštite

Objekti - Nalaženje odgovora na pitanje *Šta štititi?* je prvi ključni korak u izučavanju i razrešavanju problema zaštite u informacionim sistemima. Jer, ukoliko je skup odgovora na postavljeno pitanje prazan skup, otpada i svaka potreba preduzimanja bilo kakvih aktivnosti na ovom planu. Međutim, kako je jedan od osnovnih kri-terijuma kod utvrđivanja objekata zaštite njihova vrednost za onog kome pripada-ju, jasno je da taj skup sigurno neće biti prazan. Naprotiv, u svakom informacio-nom sistemu postoji čitav niz objekata čije vrednosti nedvosmisleno nameću pot-rebu njihove zaštite. U tom smislu niže je naveden, sa stanovišta zaštite, jedan skup tipičnih objekata: **podaci**, **datoteke**, **baze podataka**, **optičke slike dokumenata**, **digitalni zapis zvuka i slike**, **softver**, **programi**, **komunikaciona oprema**, **hardver računara**, ...

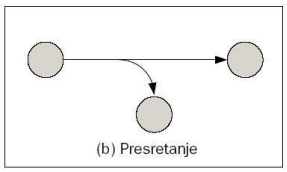
Pretnje - Na pitanje O *d koga* ili *Od čega štititi?* dobićemo odgovore koji sadrže sve klasične rizike, kao što su vatra, voda, eksplozija, računarski kriminal, greške i druge, ali i specifične pretnje, kao što je kompromitujuće elektromagnetno zračenje. Ovi specifični rizici najčešće imaju nematerijalno poreklo, ili manifestaciju, što dokazivanje njihovog postojanja, kao i procenu mogućih gubitaka, čini vrlo teškim. Određenu teškoću predstavlja i neograničen broj pretnji koje mogu ugroziti informacioni sistem, pa ih je i nemoguće sve predvideti. Među pojedinim pretnjama postoji određena međuzavisnost koja usložava uticaj na informacioni sistem.
Pretnje koje su usmerene na ugrožavanje sigurnosti toka informacija u računarskim sistemima i mrežama generalno se mogu klasifikovati u četiri osnovne kategorije.[3]



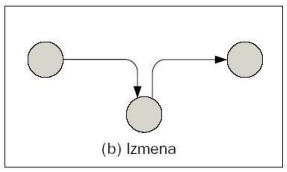
• **Presecanje** , tj. **prekidanje** (engl. *interruption*) predstavlja napad na **raspoloživost** (engl. *availability*). Presecanjem se prekida tok informacija, tj. onemogućava se pružanje neke usluge ili funkcionisanje nekog sistema. Ovakav napad je aktivan.



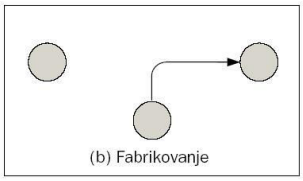
• **Presretanje** (engl. *interception*) predstavlja napad na **poverljivost** (engl. *confidentiality*). Presretanje može biti u praksi sprovedeno kao prisluškivanje saobraćaja, nadziranje njegovog intenziteta, uvid u osetljive informacije ili slično. Kao pasivan napad, teško se otkriva jer ne menja podatke tj. ne utiče na unutrašnje funkcionisanje sistema. Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.



• **Izmena** (engl. *modification*) predstavlja napad na **integritet** (engl. *integrity*). Po svojoj prirodi, to je aktivan napad. Dešava se na prenosnom putu ili unutar nekog računarskog sistema kada se radi se o izmeni podataka, pristupnih prava, načina funkcionisanja programa ili sistema i slično. Iako menja podatke ili sistem, napad često ostaje neprimećen izvesno vreme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.



• **Fabrikovanje** (engl. *fabrication*) predstavlja napad na **autentičnost** (engl. *authenticity*). Napadač izvodi ovaj aktivni napad tako što generiše lažne podatke, lažni saobraćaj ili izdaje neovlaštene komande. Veoma često se koristi i lažno predstavljanje korisnika, usluge, servera, Web strane ili nekog drugog dela sistema.



Posledice - Odgovorom na pitanje *Zbog čega štititi?* utvrđuju se negativne posledice koje identifikovane pretnje mogu da izazovu. Neke katrgorije ovih posledica su: delimično ili potpuno oštećenje, otuđenje, modifikacija hardvera i softvera, otkrivanje podataka, prekid rada sistema, ... Sve ovo utiče na povećanje gubitaka a treba smanjiti gubitke izazvane navedenim pretnjama.

Mere - Na pitanje *Čime štititi?* dobijamo identifikaciju svih mera koje stoje na raspolaganju u izgradnji celovitog i pouzdanog sistema zaštite. Sve te mere, po svojim prirodnim svojstvima koja ih karakterišu, mogu se razvrstati kao:

Mere ***normativnog karaktera***, - *pravne, organizacione i kadrovske mere,* pripadaju kategoriji *netehničkih* mera. Osnovna karakteristika ovih mera je da ne degradiraju rad sistema, već znatno doprinose povećanju njegove raspoloživosti i produktivnosti, a istovremeno značajno utiču na efikasnost sistema zaštite (npr. prava pristupa i korišćenja podataka).

Fizičko-tehničke mere uslovljavaju ih finansijske investicije pre nego što počnu da dejstvuju, tj. unapred, plus troškove njihovog tekućeg održavanja. Ovakvi troškovi se mogu tačno proceniti i izbor planski podesiti raspoloživim finansijskim mogućnostima. Ipak efikasnost ovih mera opada kada normativne mere nisu

primenjene na adekvatan način (npr. fizičko obezbeđenje IS, restriktivni prostor, Faradejev kavez, kripto urđaji i slično).

Logičke mere su snažno sredstvo zaštite. Visok stepen efikasnosti se postiže korišćenjem logičkih mera "u paketu". S druge strane, ove mere povlače za sobom tzv. prikrivene troškove, jer direktno utiču na smanjenje raspoloživosti i efikasnosti računarskog sistema, a to je dovoljan razlog da se njihovoj primeni pristupi krajnje odgovorno, osmišljeno i racionalno.

Kriptološke mere zaštite predstavljaju veoma značajne mere i u kombinaciji sa merama zaštite od kompromitujućeg elektro-magnetnog zračenja omogućavaju ostvarivanje visokog nivoa zaštite. Međutim, ove mere nisu dovoljne da samostalno obezbede potrebnu zaštitu zato što efikasnost ovih mera značajno opada ako normativne mere nisu primenjene adekvatano.

Politika - Glavno pitanje je *Kako štititi?* a to znači utvrđivanje strategije za upravljanje rizikom u ambijentu informacionih sistema. Radi toga pristupa se procesu analize i procene rizika.