Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

3. OKVIRI,METODOLOGIJE I MODELI SISTEMA ZAŠTITE INFORMACIJA

Ciljevi

Razumeti i naučiti:

– strategiju i metodologije za razvoj programa/SZ
– modelovanje procesa, komponenti i sistema zaštite
– model, prednosti i nedostatke *reaktivne* zaštite
– model, prednosti i nedostatke *proaktivne* zaštite
– model, prednosti i nedostatke *prediktivne* zaštite
– metod **bezbednosne kategorizacije i klasifikacije** IS

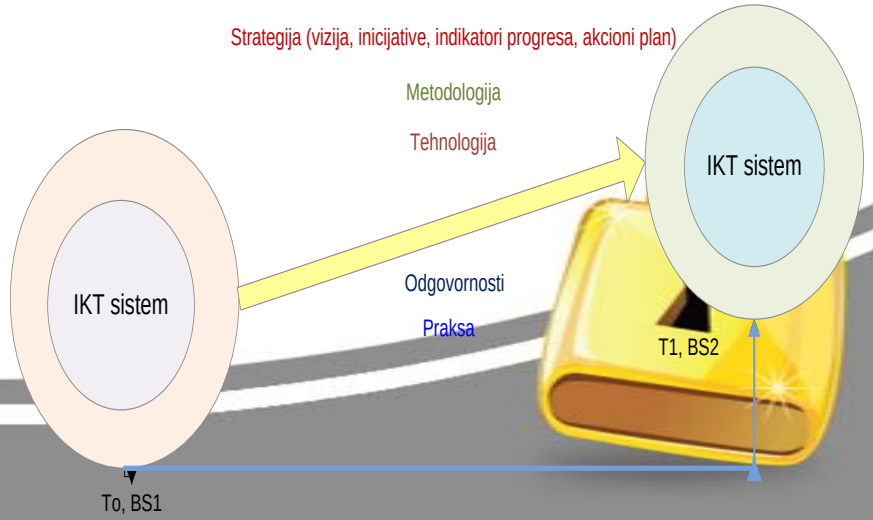
Strategija zaštite

1. Obezbeđuje:

- **Angažovanje svih resursa** organizacije
- **interoperabilnost, razvoj** SDLC **SZ** i **smernice** za procese z.
- **Okvir** za razvoj SZ za *dugoročne bezbednosne ciljeve*
- **Konsolidovanu viziju** *tekućeg i željenog bezb. stanja*
- **Inicijative** za dostizanje željenog stanja
- **Sistem indikatora** za praćenje progresa (*benchmark*)
- **Akcioni plan** za izvršavanje strateškog cilja

2. Realizuje se konceptima:

- *metodologije,*
- *tehnologije i*
- *operativne prakse zaštite*



Ključni koncepti za razvoj sistema zaštite

Koncepti	Primeri realizacije
Metodologija	*Principi*: GAISP *Modeli*: IKTS, procesa, arhitekture sistema zaštite itd. *Metodi:* kvantitativni, kvalitativni; standardi najbolje prakse. *Razvoj procesa:* procena rizika, SE; plan zaštite …
Tehnologija	*Alati:* hardversko–softverski; *Tehnike*: manuelne, polu-automatske, automatske *Tehničke kontrole:* hardversko/softverski mehanizmi i protokoli.
Prakse zaštite	*Operativne kontrole*: aktivnosti proceduralne zaštite.
Odgovornost	*Upravljačke kontrole*: pripisivanje odgovornosti za zaštitu.

Okviri i metodologije

1. **Definišu se na osnovu** *internih i/ili industrijskih standarda*
2. **Grupišu se zajedno** *u SMFi dodaju strukturu procesima z.*

PRIMERI *metodologija* *(uslovna podela)*:

- *ISO/IEC 27005, NIST SP 800-30* - za analizu rizika
- *CC*-opšti kriterijumi za evaluaciju proizvoda/SZ
- *ISO/IEC 27001* – menadžment sistem zaštite inf.

PRIMERI *okvira/modela* *(uslovna podela)*:

- *ISO/IEC 21827* (*SSE CMM*) – model zrelosti procesa z.
- *ISO/IEC 27002* - za izbor kontrola zaštite (SMF) itd.
- NIST SP 800 – XY serija peporuka

Tehnologije zaštite

1. **Tehničke kontrole zaštite:**

– **Izvršavaju ih hw/sw mehanizmi** i **protokoli** zaštite

– **Obezbeđuju**:

- *upravljanje identitetom* (IAA*)
- *kontrolu fizičkog i logičkog pristupa* RS/RM...
- *kriptozaštitu informacija* (datoteka, direktorijuma...)
- *detekciju/sprečavanje upada u sistem* (IDPS)
- *kontrolu saobraćaja u RS/RM* (skeneri) i dr.

IAA*- Identifikacija, Autentifikacija, Autorizacija

Praksa zaštite

2. Organizaciono-operativne kontrole:

- **Izvršavaju ih uglavnom ljudi** koji obezbeđuju:
  - izvršavanje procedura zaštite
  - maksimizaciju upravljačke i operativne efektivnosti i efikasnosti IKTS
  - personalnu, fizičku i zaštitu od uticaja okruženja
  - upravljanje vanrednim događajima i incidentom
  - upravljanje promenama (konfiguracijom sistema)
  - održavanje, obuku i razvoj svesti o potrebi zaštite...

Odgovornosti u zaštiti

3. ISMS i upravljačke kontrole:

- **pripisuju odgovornosti svim zaposlenim**
- **minimiziraju legalne posledice**
- **maksimiziraju praksu zaštite kroz**:
  - procenu rizika, planiranje zaštite
  - akviziciju sistema/servisa zaštite
  - analizu *kontrola zaštite*, autorizaciju prava pristupa
  - sertifikaciju i akreditaciju sistema zaštite…

Sistem inženjerski razvoj S/Z

1. **Proces zaštite (SE):**
   - **skup** ljudi, sredstava, povezanih aktivnosti za postizanje jedinstvenog cilja... (IEEE)
   - **transformator** ulaznih parametara u SZ u izlazne…
   - **integrator** *ljudi, tehnologija, procedura/metoda*
2. **Procedura zaštite*:***
   - povezuje **U** i **O** aktivnosti *zaštite*
   - *određuje* redosled aktivnosti i dokumentuje proces z.
2. **Projekat zaštite**:
   - skup konačnih procesa i resursa (ljudi, vreme, tehnologije, finansije) namenjenih za dostizanje jedinstvenog cilja zaštite

Metodologija i modeli za razvoj sistema zaštite

Opšta metodologija za razvoj programa/SZ

<u>Metodologija SDLC</u> (za razvoj ž/c) na bazi:

1. **upravljanja rizikom**
2. **politike zaštite**
3. **standarda najbolje prakse zaštite:** (*ISO/IEC 27K, ISO/IEC 21827, NIST SP 800-30, NIST SP 800-53,...*)

Realizuje koncepte**:**

1. *reaktivne zaštite,* od *poznatih* napada.

2. *proaktivne* zaštite, od *poznatih* i *nepoznatih pretnji*

3. *prediktivne* (*smart*) zaštite

Strukturno modelovanje SZ

1. **Skup objekata s/z**:
   – *pasivnih* (*aktivnih*) kojima se pristupa na kontrolisan način
2. **Skup subjekata s/z** :
   – *aktivnih* komponenti koje koriste i pristupaju objektima
3. **Skup pravila**:
   – kako **subjekti koriste i pristupanju objektima**
   – za **dekompoziciju** (klas./kateg.) objekata na skupove, prema definisanim kriterijumima (ciljevi, funkcije z. itd.),
   – **odbacuje nebitne komponente** i smanjuje kompleksnost

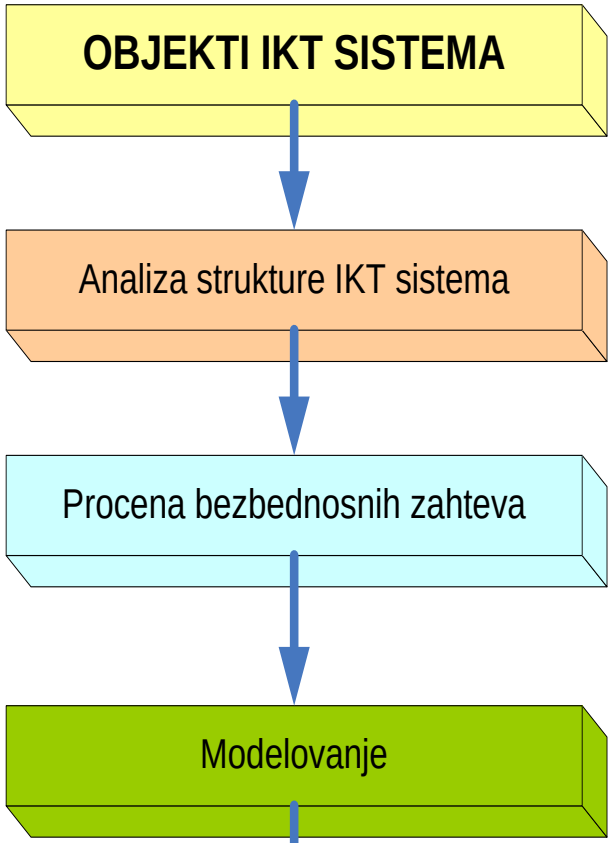
- **Obuhvata** bezbednosno relevantne objekte IKTS:
  – *CAOP, LAN, maliciozni napadi, udaljeni korisnici...*

Primeri primene strukturnih modela

Primer: modelovanja sistema osnovne zaštite IKTS

Modelovanje IKT sistema:

- *Modelovanje mehanizma logičke kontrole pristupa*
- *Strukturno modelovanje mrežne IKT arhitekture*



Primer: Strukturni model LAC

Strukturni model mehanizma logičke AC (LAC)

- Model definiše bezbednosno stanje sistema matricom pristupa – (***M***)
- **M** : redovi – ***subjekti*** (***S***), kolone – ***objekti*** (***O***),
- **Ćelije M:** atributi pristupa (***A)***, ili ovlašćenja za pristup i korišćenje ***O*** od strane ***S***
- **Ćelije M možemo definisati** sa:

M(S,O)=A

- što označava da subjekat **S** ima prava pristupa i korišćenja tipa **A** na objektu **O**

Primer: Strukturni model LAC

- **Referentni monitor:**
  - poseban kontrolni program za pristup **S** do nekog **O**
  - pridružuje se svakom **O** u sistemu
  - subjekat **S** zahteva pristup do objekta **O** na način **a**
  - OS kreira trojku **(S,O,a)** i dostavlja je programu referentnog monitora za objekat **O**
  - monitor upoređuje atribute pristupa **A(S,O)** iz matrice pristupa, primenjujući zahtev **a**
  - ako je **a** atribut, pristup je dozvoljen, ako ne - odbija se

Primer: Strukturni model arhitekture RM

- ***Strukturni model mrežne arhitekture :***
  - obezbeđuje **smanjenje kompleksnosti**:

    1.korak: analiza dokumenta mrežnog plana i uklanjanje svake neophodne informacije

    2. korak: ažuriranje mrežnog plana sa stvarnim stanjem topologije mreže

    3. korak: određivanje *kategorija bezbednosnih zahteva* za svaku grupu

    4. korak: grupisanje istih ili sličnih kategorija bezbednosnih zahteva u zajedničku ***zonu bezbednosti***.

PRILOG I 3D.doc

Nedostaci strukturnog modelovanja

1. **Zastareo** zbog podele na aktivne (***S***) i pasivne (***O***)
   – svaki program realizuje konkretni korisnik:
   – realizacija objekta (**O**) je složena
   – objekat ispunjavava volju korisnika (**S**)
   – **S** direktno (po pravilu indirektno – **preko OS**) na svoj rizik zahteva od **O** određeni informacioni servis
2. **Ponovljeno korišćenje O** IKTS nije obezbeđeno
3. **Zaštita RM** – problem uspostavljanja koherentnog SZ
4. **Slabo se koriste znanja** iz OOM

OOM - Klasifikacija (K)

- **Generička definicija (*atributi klasifikacije - K*):**
  - *Međusobnu isključivost:* sprečava preklapanja
  - *Potpunost:* unija svih kategorija - sve moguće ***K***
  - *Nedvosmislenost:* jasna i precizna
  - *Ponovljivost:* ponovljiva, daje isti rezultat
  - *Prihvatljivost:* logička i intuitivna
  - *Primenljivost:* primenljiva u različitim oblastima

OOM - Klasifikacija (K)

- **Klasa*:*** apstrakcija skupa realnih karakteristika ***O,*** objedinjenih *opštom strukturom i ponašanjem*

  Primer: klasa -„*korisnik*“, objekat - „*korisnik XY*“
- **Objekat*:***
  - *elemenat klase*, tj. apstrakcija određene stvarnosti,
  - *aktivni element* sa *unutrašnjom strukturom i ponašanjem*
- **K** svih ***O* informacione imovine** u bezbednosne kategorije (***BK***), na *koje* su primenljivi svi navedeni atributi ***K:***

  Bk = (Bk P) (Bk I) (Bk R) = (N) (S) (**V**) = **V**

  Primer: **klasifikacija informacija** prema bezbednosnim nivoima - *interne, službene, poverljive* informacije

OOM - Metodologija

- **Svi elementi sistema** su ravnopravni objekti (**O**)
- Nema pasivnih **O**, **svi O su aktivni**
- Struktura IKTS/SZ **dekomponuje se na O**
- **O** po potrebi izazivaju načine ponašanja (*metode*) jedan drugoga
- Realizacija ponašanja je skrivena (*inkapsulirana*):
  - **vidljivi su samo interfejsi** (smanjuje kompleksnost!)
- **O** međusobno povezuju samo **interfejsi**

Atributi OOM

1. **Inkapsulacija:**
   - *smanjuje kompleksnost*, skraćuje strukturu/ponašanje **O**
   - vidljivi samo određeni interfejsi
   - **označava „*relativnu nezavisnost*“** svake *grane*
2. **Polimorfizam:**
   - sposobnost **O** da se svrsta **u više od 1 klase**

     Primer: korisnici SZ u različitim ulogama (adm., korisnici)
3. **Nasleđivanje*:***
   - formira novu klasu ***O*** iz postojeće-**dodaje podatke**
   - smanjuje ponovljive elemente SZ-**ukazuje na promene**
   - klasa-*potomak* - **koren nove klase**-*naslednika*
   - sledeći nivo zaštite se ne menja-**dopunjuje prethodnim**
   - omogućava primenu ***slojevitog koncepta*** *zaštite*
4. **Nasleđivanje + polimorfizam** = modularna skalabilnost

Atributi OOM-1

5. Grana objekta - *relativno nezavisnih* (ortogonalnih) skupova **O**

- *omogućava raznolikost* aspekata apstrakcije **O**

a. Skup grana O informacione imovine:

- struktuira **bezbednosni cilj – zaštita *CIA*** informacija

b. Skup grana objekata S*I*Z: struktuira sredstva - **U,O,T** k/z

- **Daju 12** *kombinacija* (**3! +3!)** - prihvatljiv kompleksnost

6. Nivo dekompozicije - *hijerarhijske forme*:

- važan za vizuelizaciju i SA složenih **O**
- *algoritam dekompozicije*:
  - prvi nivo hijerarhije se razmatra sa nivoom detalja ***n >0***,
  - sledeći se razmatra sa ***(n-1),*** sledeći - ***(n-2)...***
  - poslednji se razmatra sa nivoom detalja ***(n-n)=0***
  - **O** sa **n. detalja *0*** smatra se nedeljivim (**atomizovan**)
  - nivoi detaljizacije variraju za **O** i **grane objekta**

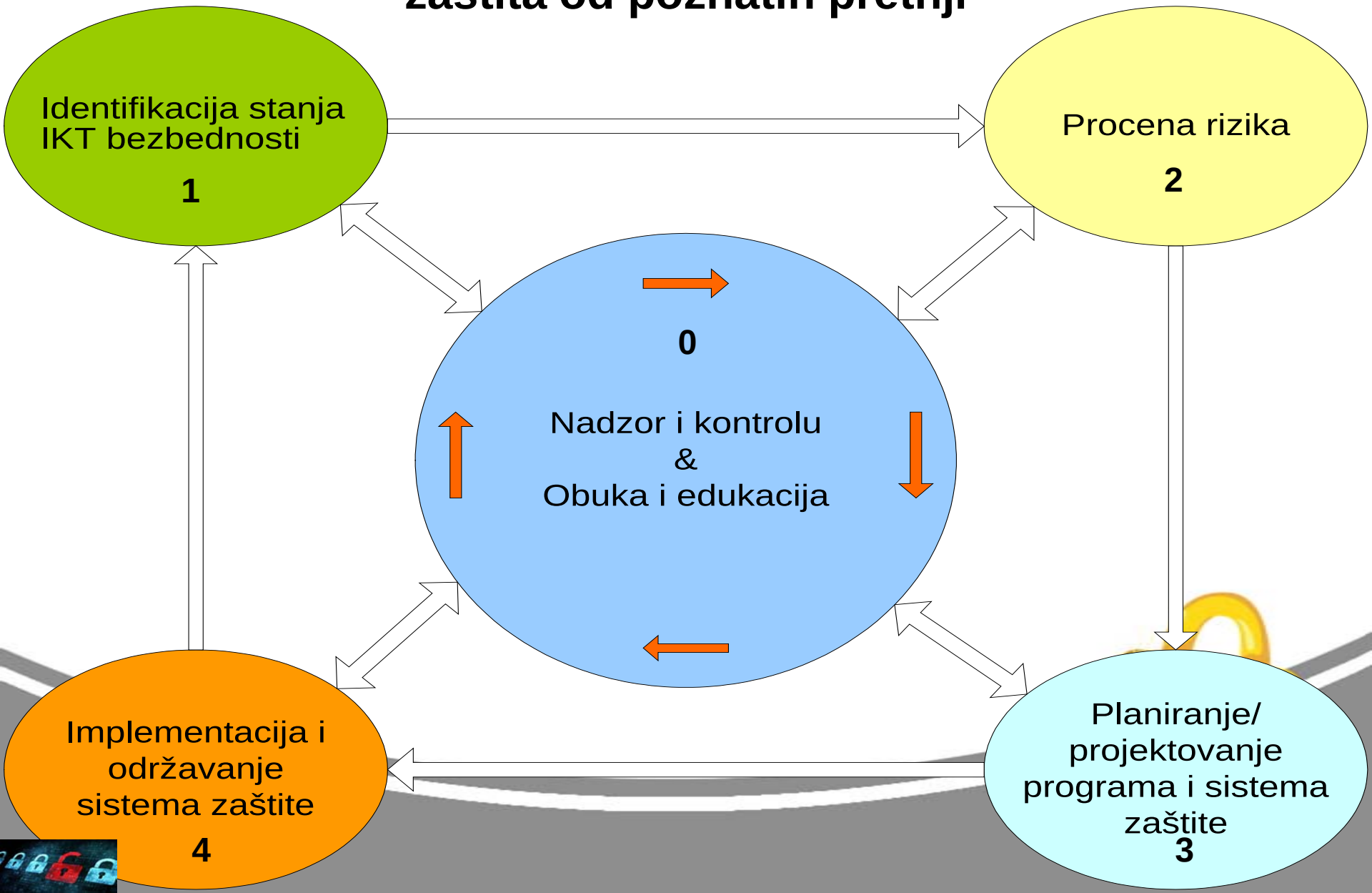
Primer: OOM sistema zaštite

- Fiksna grana ***raspoloživost*** zahteva sve elemente drugog skupa (**U,O,T k/z**);
- Fiksna grana ***integritet*** zahteva sve elemente drugog skupa (**U,O,T k/z**);
- Fiksna grana ***poverljivost*** zahteva sve elemente drugog skupa (**U,O,T k/z**)

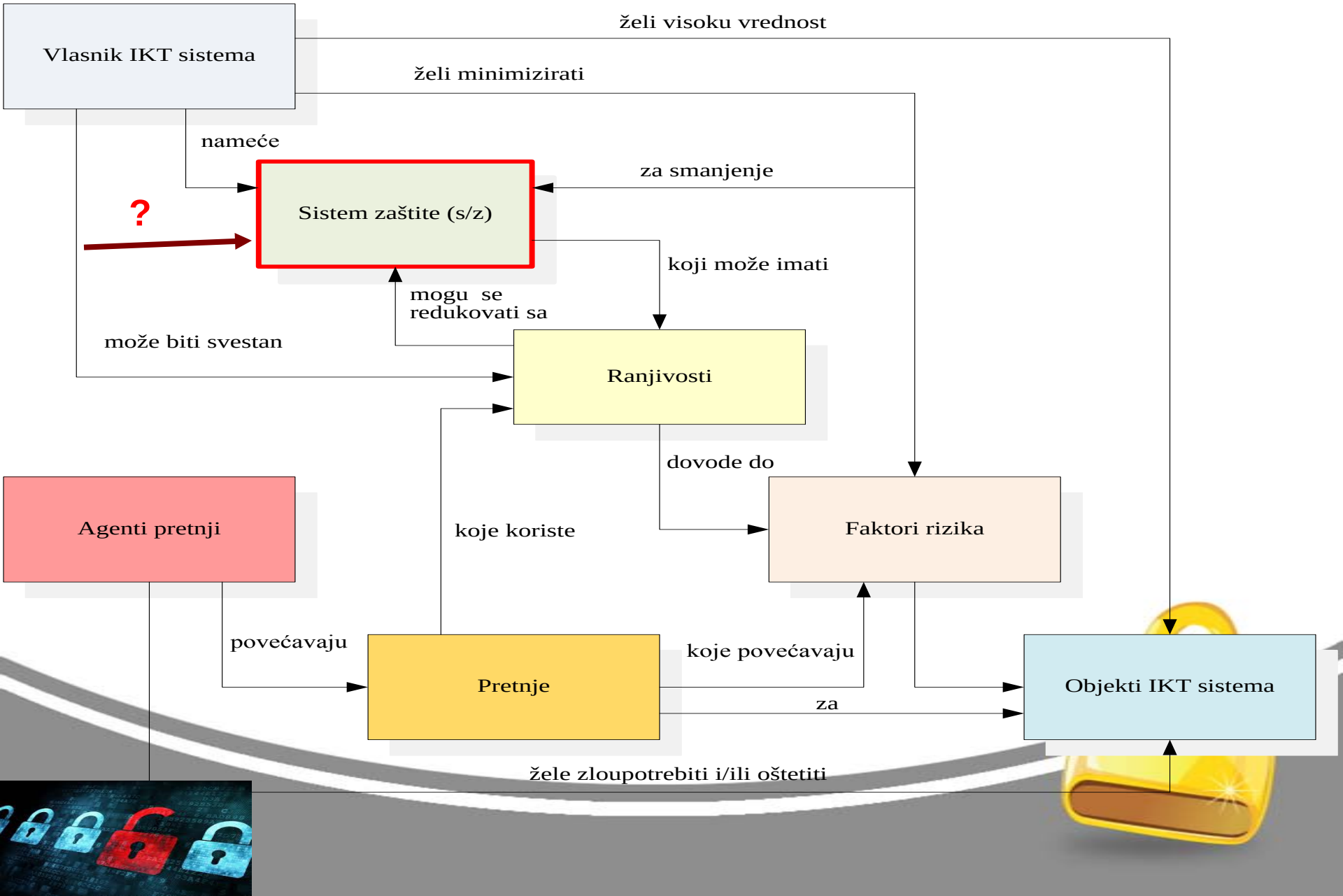
Koncepti sistema zaštite

1. Reaktivni sistem zaštite
2. Proaktivni sistem zaštite
3. Prediktivni sistem zaštite

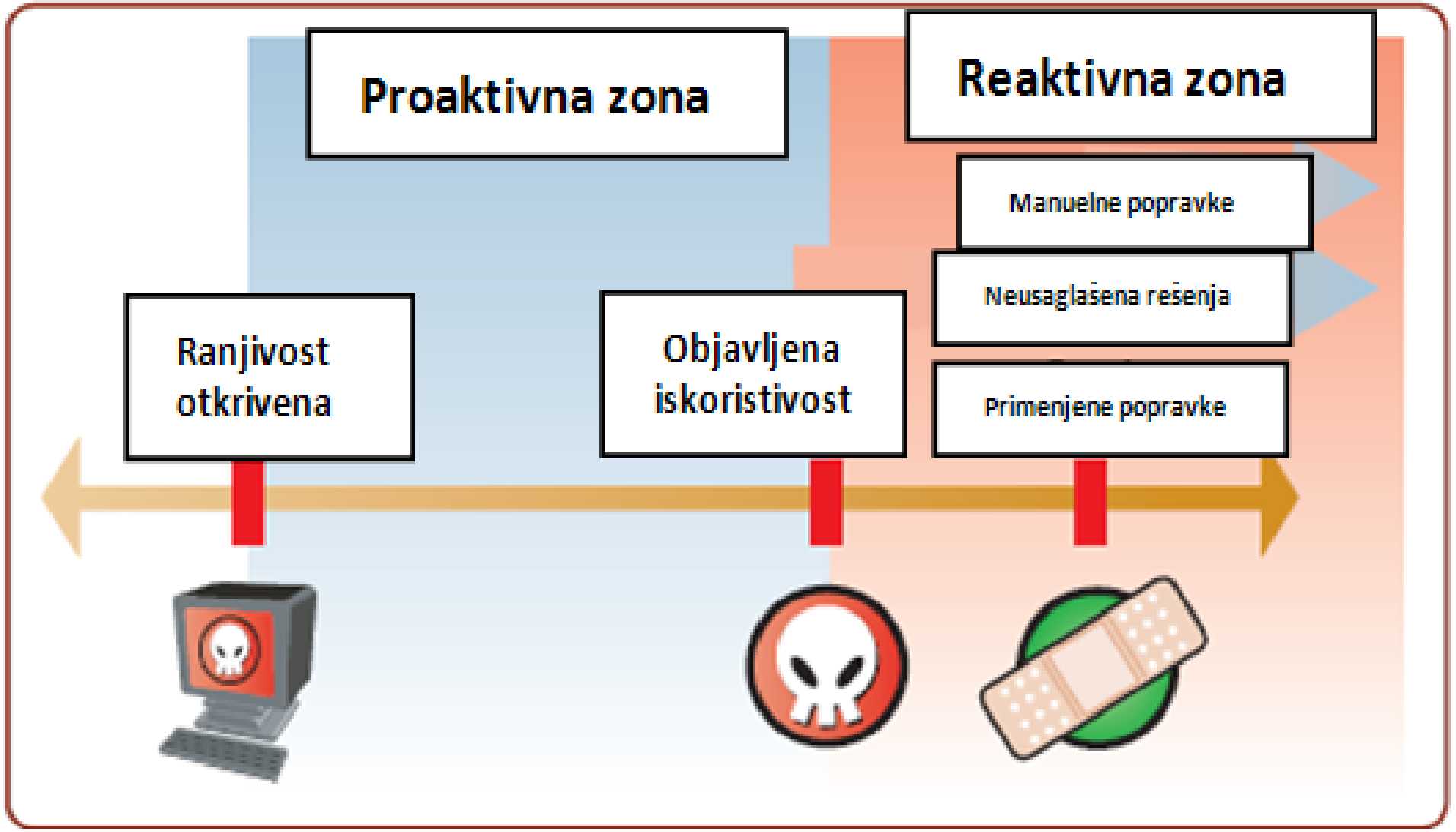
Funkcionalni model reaktivne zaštite
-zaštita od poznatih pretnji-



Generički model reaktivnog sistema zaštite



Primer: Zona zaštite reaktivnog sistema



Proaktivni sistemi zaštite

1. **Koristi mehanizme** *proaktivne zaštite* **na više nivoa**:
   - *različitih brzina reakcije i preciznosti (adaptivne!)*
   - *veće ukupne efektivnosti/efikasnosti*
   - *za detekciju i odgovor na poznate i nepoznate napade*
   - *smanjuje operativni rizik i troškove*

Proaktivni sistemi zaštite

Realizacija *proaktivne zaštite*:

1. **ažurna baze znanja i podataka** o napadima i ranjivostima (**CIRT/CERT**)
2. **vodeće tehnologije proaktivne zaštite** *za*:
   a. detekciju napada,
   b. proaktivnu zaštitu od *poznatih* i *nepoznatih* pretnji **(***virtual patch***)**
   c. adekvatni odgovor na napad
3. **pojednostavljen proces zaštite**

1. Proktivni sistem zaštite -*baza znanja*

- ***ISC CBK, NIST, ISF, ISS*** (*10-12 komponenti zaštite):*
  - upravljanje, arhitektura i modeli sistema zaštite
  - kontrole pristupa, zaštita razvoja aplikacija
  - operativna, fizička i kriptografska zaštita
  - plan kontinuiteta poslovanja (upravljanje VD i incidentom)
  - akreditacija i sertifikacija sistema zaštite
  - istraga zloupotreba IKTS (zakonski okvir, etičke norme)
- ***katalozi kontrola dobre prakse zaštite:***
  - ISO/IEC 27002, *NIST SP 53a,b,c; ISFv.4; QUALIS…)*

2. Proaktivni sistem zaštite-*tehnologije*

Primer: IBM/ISS tehnologija proaktivne zaštite

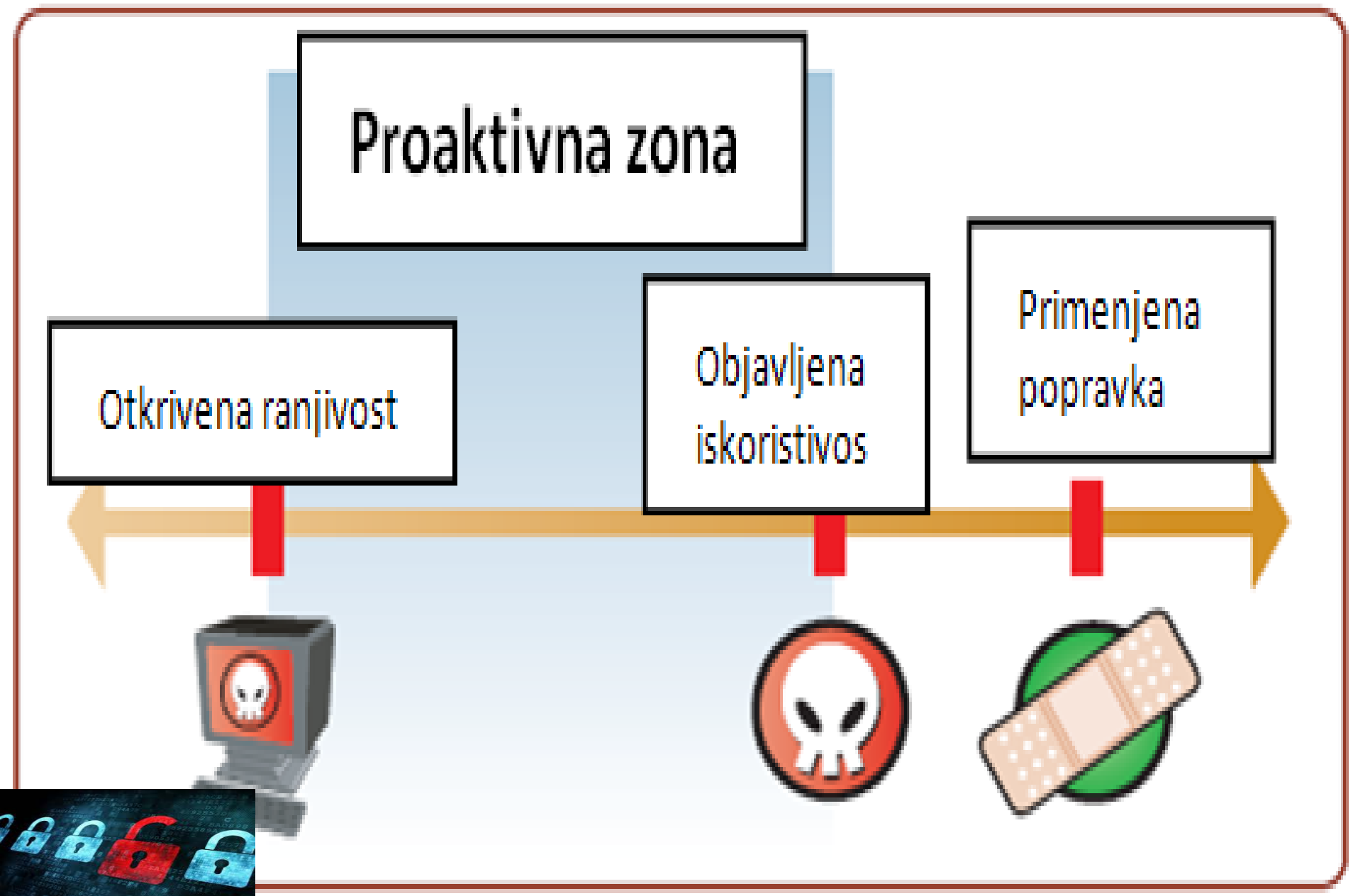
- **Centralnu jedinicu zaštite (*Protection engine*):**
  - *IDPS*, *Protection Engine*, reaktivni modul
- **Komandnu jedinicu (*Site Protector*)**
  - kontrolne komande, centralizovano upravljanje
- **Integrator sistema (*Fusion System*):**
  - digitalnu obradu signala, prepoznavanje obrazaca napada, analizu uticaja DPP napada
- **Modul za ažuriranje** *(X-Press Updater*):
  - automatski ažurira bazu podataka *napada* i *ranjivosti*

Proktivni sistem zaštite-proces zaštite

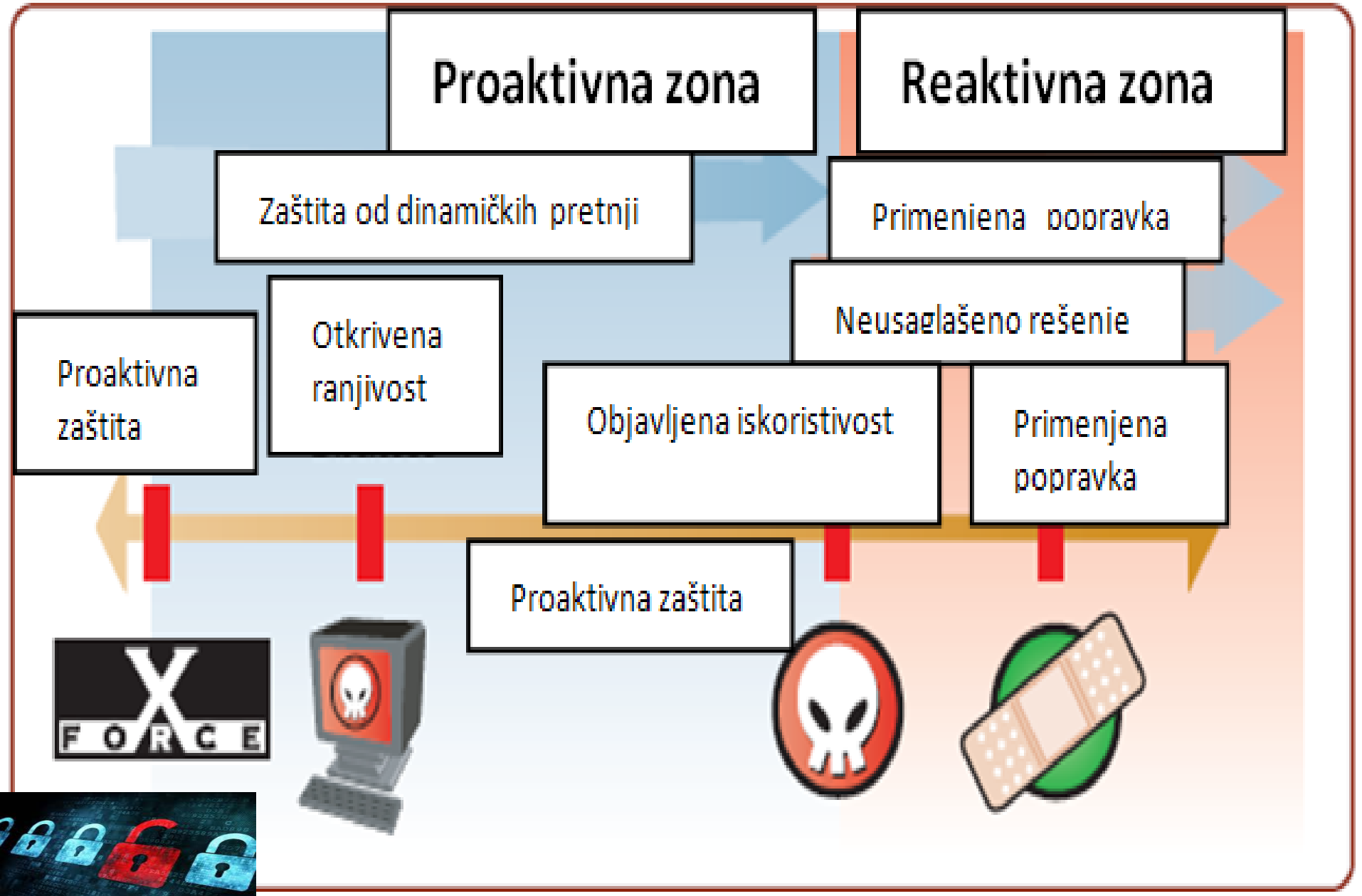
- **Virtuelna bezbednosna popravka *(Virtual Patch*):**
  - automatski sanira otkrivene ranjivosti sistema
  - sanira ranjivosti pre generisanja i objavljivanja zakrpa
  - u realnom vremenu štiti od *poznatih i nepoznatih napada*
  - preventivno održava sistem zaštite
  - redefiniše koncept održavanja/upravljanja SZ u:
    - *deo procesa upravljanja promenama IKT sistema*
    - *deo TQM procesa*
  - obezbeđuje efektivnije/efikasnije planiranje resursa

Primer: QUALIS *Cloud Computing* servis zaštite inf. imovine

Primer: zona proaktivne zaštie



Primer: proširena zona proaktivne zaštie



Trend razvoja IKTS

- **Trend sledećih 5 g.a (Gartner, 2009)**:
  - virtuelizacija kijenta i servera (*Cloud Computing*)
  - manja potrošnja energije (*ekološko računarstvo*)
  - praćenje resursa
  - primena društvenih mreža (*facebook* i dr..) i na radnom mestu**??**
  - unifikacija komunikacija, jeftine aplikacije…
- **Potreba da se redefinišu koncepti sistema zaštite:**
  - *nova pardigma zaštite*

Novi koncept zaštite

- **Predlog 7 glavnih principa zaštite** (RCA London, 2009):
  1. Sistem zaštite se mora **ugraditi, a ne integrisati** u IKTS (npr. *CISCO e-mail security gateway*)
  1. Razvoj **ekosistema zaštite** (npr. *finansijske institucije*)
  2. Kreirati **koherentni i transparentni SZ** za korisnike (*e-plaćanje*)
  3. Obezbediti **centralizovano upravljanje i korelaciju incidenata**
  4. Sistem zaštite mora biti **orijentisan na zaštitu spolja i iznutra**
  5. Sistem zaštite mora biti **dinamičan i zasnovan na proceni rizika**
  6. **Samoobučavajući** sistem zaštite (npr. **proaktivno prikupljanje informacija** o špijunima, virusima, spamu itd.)

Politika zaštite
-Definicija-

- **metodološki najznačajnija komponenta s/z**
- **izjava na visokom nivou relativno nepromenljiva!?**
- **smernice** org. za program/sistem zaštite
- **sadrži specifična pravila** - izjave, saopštenja
- ključna komponenta plana zaštite
- **okvir** očekivanja,obaveza, tehnologija i procesa
- **utvrđuje ciljeve**, očekivanja i odgovornosti
- **koristi:** *instrukcije, procedure, uputstva, pravce aktivnosti i principe* zaštite

Politika zaštite
-Funkcije-

- **okvir za donošenje odluka** u oblasti zaštite
- **adaptivna -** kroz procedure i uputstva
- **sadrži standarde**, najbolju praksu i preporuke za arhitekturu s/z i evaluaciju usaglašenosti
- **referenca (***benchmark)* za:
  - legalnu zaštitu od odgovornosti (?)
  - dokazivanje pred sudom u slučaju k. kriminala
- **nametanje prakse zaštite:**
  - obezbeđuje ***osnovu za disciplinske mere***

Politika zaštite
-Struktura i vrste-

1. Struktura (opšta):

- uvod
- saopštenja (jasna, koncizna): *funkcionalna, odgovornosti*
- zahteve za usklađenost i monitoring
- komponente prinude (**sankcije**)
- kontaktne informacije (vlasnika)

2. Vrste:

- ***programska (****na nivou organizacije****)***
- ***funkcionalna (****za specifične radne funkcije****)***
- ***IKTS***
- ***ISMS politika za upravljanje zaštitom informacija*** *(Information Security Management System)*
- ***komponenti zaštite*** *(npr. Politika udaljenog pristupa)*

Programska politika zaštite (NIST)

- **Obuhvata osnovne instrukcije za**:
  - bezbednost rada organizacije i zaštitu informacija
  - prihvatljivo korišćenje tehnologije zaštite
  - upravljanje bezbednosnim rizikom (UR),
  - upravljanje VD i kompjuterskim incidentom i
  - obezbeđenje kontinuiteta poslovanja

  Primer: Menadžment rizika
  - definiše cilj, obim i *odgovornosti*
  - sugeriše izbor metoda analize i procene rizika
  - zahteva nadzo/kontrolu procesa UR (*usaglašenost...*)
  - odobrava nivo prihvatljivosti preostalog rizika

Funkcionalna politika zaštite (NIST)

- odnosi se na **specifične *radne funkcije organizacije***
- navodi razloge zašto je politika potrebna
- opisuje funkcije koje pokriva (**ZIS, FINIS, IS e-Uprave**)
- definiše odgovornosti i kontakte
- obezbeđuje „*balans zaštite i produktivnosti*“
- određuje prioritet zaštite u odnosu na funkciju CIA
- predlaže sankcije i tretman povreda politike

Primer: *Politika zaštite zdravstvenog IS (ZIS)*

  - podaci/informacije raspoložive za lekare/med.sestre/laboratoriju
  - podaci/informacije posebno zaštićene
  - podaci/informacije specificirane za pristup/rukovanje određenim licima
  - definiše način šifrovanja podataka/ informacija i destinacije slanja

Politika zaštite IKT sistema (NIST)

- **Uspostavlja *standarde* za bezbednosno okruženje IKTS**:
  - obezbeđenje pouzdanosti rada uređaja i mrežnih servisa
  - namenu zaštitnog softvera za okruženje hosta
  - uspostavljanje standarda Kz za radne stanice (PC i LapTop)
  - specifikaciju zahteva za upravljanje VD i k. incidentom
  - bekapovanje i oporavak sistema, kontinuitet poslovanja i dr.

Primer: *Politika upravljanja konfiguracijom (promenama) IS*

- definiše metode testiranja novog hw/w,
- definiše metode instalacije i neophodnu dokumentaciju,
- sugeriše proces upravljanja svim promenama i
- identifikuje pravo ***vlasništva*** nad sistemom
- definiše ovlašćenja za izmenu konfiguracije

ISMS politika zaštite

- Definisana standardmo ISO/IEC 27001
- Može biti samo za upravljanje s/z (krovna) ili zajedno sa politikama komponenti s/z
- Sadrži sve standardne elemente
- Pokazuje odluku menadžmenta organizacije da uspostavi ISMS
- Može biti javna

Politika komponenti sistema zaštite

- **Obezbeđuje zahteve za operativno upravljanje s/z:**
  - upravljanje pasvordom
  - autentifikaciju i autorizaciju
  - nadzor i kontrola (*audit*) sistema zaštite
  - upravljanje incidentom i VD, e-poslovanje
  - oporavak sistema ....
- **Primer: *Upravljanje kompjuterskim incidentom***
  - definiše **ko/kako** upravlja incidentom i vrši istragu napada
  - kako/kada se interni/eksterni napad dogodio
  - **ko** objavljuje incident, **kome** dostavljati izveštaj
  - **ko/kako** vrši **forenzičku istragu** digitalnih dokaza

Primer: Prilozi\POLITIKA KONTROLE PRISTUPA.doc

Metodologija izrade *politike zaštite*

- **Standardi za izradu *politike zaštite***
  - ***ISO/IEC 27001, ISO/IEC 13335 TR-3, NIST*** SP 800 -12,18, 30
- **Praktični principi - obezbediti:**
  - »bezbednost« greške (*sistem bezbedan i kad dođe do greške)*
  - evidentiranje bezbednosnih događaja
  - jednostavnost rešenja arhitekture sistema zaštite
  - **minimizaciju privilegija i odvajanje dužnosti i privilegija**
  - nedopustivost prelaska sistema u nebezbedno stanje
  - nemogućnost zaobilaženja mehanizama zaštite
  - sveopštu podršku organizacije
  - jačanje zaštite samo slabih komponenti
  - potpunu posrednost pristupa informacijama (*proxy*?)
  - korisničku prihvatljivost i slojevita zaštite RM i RS

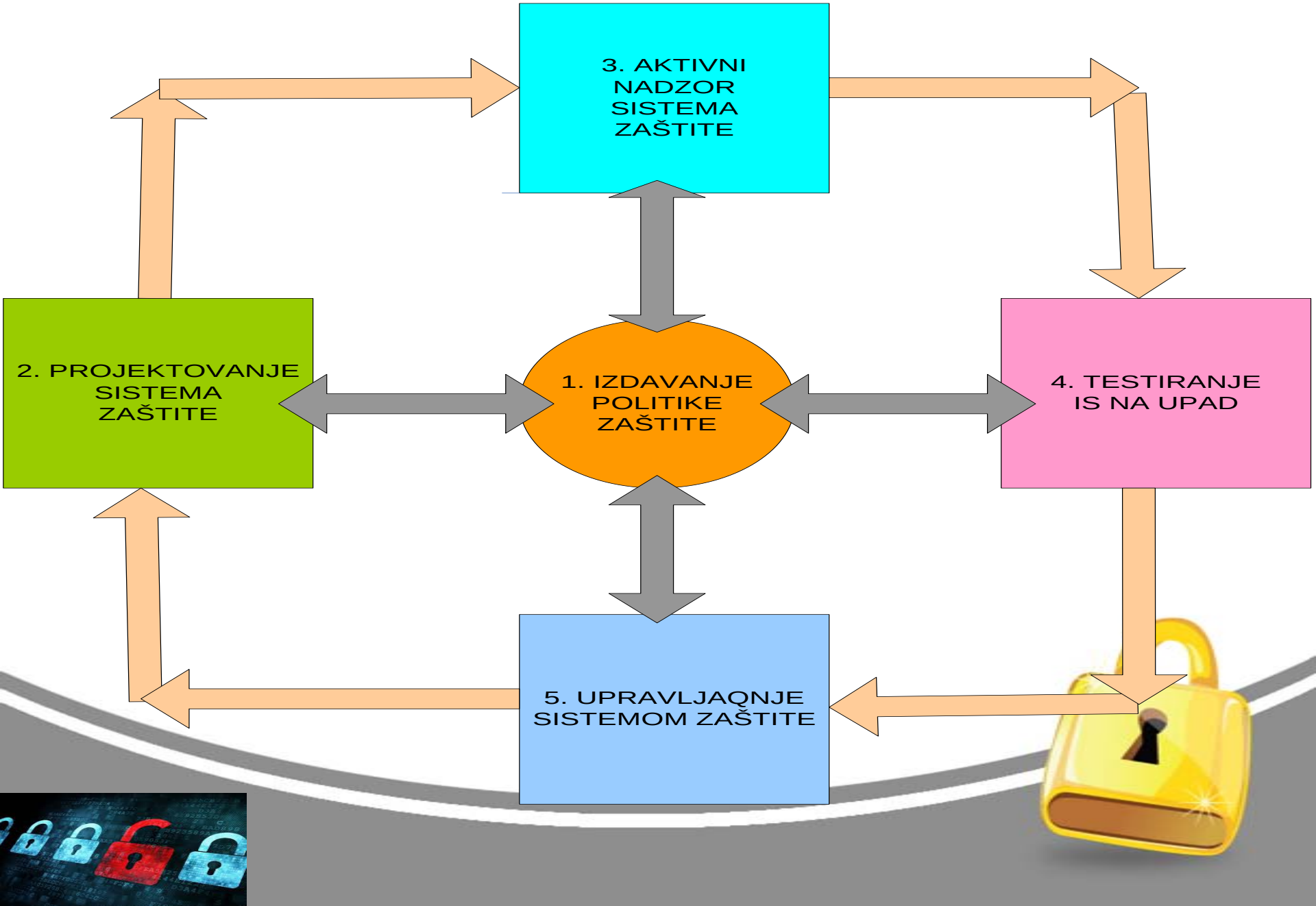
Proces izrade politike zaštite

1. **Izrada politike zaštite je autorski rad**
- **Specijalista za zaštitu formira radnu grupu od**:
  - informatičara, menadžera org. jedinica i spoljnih saradnika
- **Konačan nacrt** podnosi upravi na odobravanje i promoviše politiku

2. **Opšti model za izradu politike zaštite**
   - *Odnosi se na sve aspekte zaštite IS*
   - *Povezuje sve komponente sistema zaštite*
   - *Pripisuje odgovornost svim zaposlenim*
   - *Obezbeđuje osnov za disciplinske mere (sankcije)*
   - *Zasniva se na rezultatima procene rizika*

3. **Osnovni kriterijumi za izradu politike zaštite su:**
   - *Mogućnost dopunjavanja*
   - *Vidljivosti (transparentnosti)*
   - *Menadžerska podrškaa*
   - *Konzistentnost i eksplicitnost saopštenja*

Primer: Procesa održavanja politike zaštite



Preporuke za izradu politike zaštite

1. obezbedi **podršku upravne strukture**
2. **laka za razumevanje** i što je moguće kraća
3. **usklađena sa kulturom rada** i okruženjem
4. racionalna i **da omogućava postizanje poslovnih ciljeva**
5. obavezna i da **nameće realizaciju**
6. **afirmativno** ističe šta treba uraditi (*treba, mora,..*),
7. **izbegava** reči tipa *nikada*, *zabranjeno* i sl.
8. odnosi se na **sve klase informacione imovine**
9. uklapa se u druge politike organizacije
10. sadrži **saopštenja šta treba zaštititi** i u kom obimu
11. sadrži informaciju **kada politika stupa na snagu** i koje su **sanakcije**
12. sadrži informaciju **na koga se odnosi** i na koje std. referencira

Preporuke za izradu politike zaštite-1

13. sadrži **razloge za propisivanje** i **ko je razvio**
14. sadrži **metod kojim će se monitorisati usklađenost**
15. objašnjava **kako će biti nametnuta** i **ko je odgovoran**
16. objašnjava koja su **odstupanja dopuštena**
17. sadrži informaciju **kada će se preispitivati** i ko vrši reviziju
18. sadrži **datum poslednje revizije** i da li postoji arhiva
19. sadrži termin *elektronski* za informacije u el. formi
20. identifikuje **kontaktne informacije** za izveštavanje o k/i
21. uravnotežava nivo kontrola zaštite i nivo efektivnosti s/z
22. prilagođena veličini organizacije
23. obezbeđuje **poverenje korisnika** u komponente zaštite

Izrada *politike zaštite*

- **Izražavanje značaja politike zaštite:**
  - formira osnovu za *upravljački okvir* sistema zaštite,
  - obezbeđuje *uputstva, smernice, instrukcije*,
  - definiše *uloge i odgovornosti* u zaštiti,
  - *dokumentuje* stav organizacije u odnosu na određeno pitanje zaštite
- **Identifikovanje/definisanje saopštenja:**
  - uzorci saopštenja u bazama znanja (Internetu)
  - zavise od kulture rada i veličine organizacije
  - jednostavnija odgovaraju manjim, a preciznija–većim orgaizacijama
  - *teško izbeći preklapanja i ponavljanja*

Rešenje*: definisanje standardne strukture* **-** zajedničkih i specifičnih elemenata politike zaštite

Struktura *Politike zaštite (NIST)*

Standardni elementi

(Zaglavlje: autor, datum, verzija..)

1. *Uvod*
2. *Struktura, obim i namena*
3. *Bezbednosni cilj (1-3 tipični deo svake politike zaštite)*

Autorski deo

4. Saopštenja

4.1. (specifični funkcionalni elementi politike zaštite na različitim nivoima)

4.2. (uloge i odgovornosti svih zaposlenih u organizaciji)

5. Usklađenosti, sankcije za neusklađenost

6. Rečnik termina (ključne reči)

7. Odobrava (4-7 specifični deo svake politike zaštite)

Primer: Izrada *politike zaštite*

PRIMER: Struktura *Politika zaštite privatnosti*

1. – 3. (Tipični deo opšte strukture politike zaštite)

4. Saopštenja:

- *Uskladištene informacije*
- *Metod skupljanja informacija*
- *Upravljanje kolačićima*
- *Pristup ličnim podacima*
- *Ažuriranje ličnih podataka*
- *Zahtev za isključivanje*
- *Dostupnost za treću stranu*

5-7. Ostale informacije

Zaključci

1. **Strateški plan zaštite**: dugoročni razvoj programa zaštite, realizuje se kroz *metodologiju, tehnologiju, operativnu praksu (uključujući odgovornosti)*
2. **Metodologija** je određena definisanjem: *principa, koncepata (modela), metoda (tehnika i alata)* i *toka razvoja procesa*
3. **Opšta metodologija razvoja programa/SZ** na bazi: *politike zaštite (R)*, i/ili *upravljanja rizikom (R)* i/ili *standarde najbolje prakse zaštite (P*
4. **Model-** apstrakcija realnog sistema, strukturni i objektno orijentisani smanjuju kompleksnost sistema
5. Metodološki značaj politike zaštite

Pitanja