# Bezbjednost i zaštita informacionih sistema

# 9. Pravni, organizacioni i društveni aspekti

Prof. dr Nikola Žarić

e-mail: zaric@ucg.ac.me

# Konvencija o cyber-kriminalu

* **Vijeće Evrope** je u **novembru 2001**. **donijelo konvenciju** kojom je pokušalo **dati smjernice** u borbi protiv računarskog kriminala.
  * **krivična djela protiv tajnosti**, nepovrjedivosti i dostupnosti podataka
  * **krivična djela poput prevare i faslifikovanja** uz pomoć računara
  * **krivična djela koja se odnose na sadržaj podataka**
    * npr distribuciju i širenje uznemirujućih sadržaja
  * **kršenje autorskih i srodnih prava.**

# Konvencija o cyber-kriminalu

* Krivična djela protiv tajnosti, nepovrjedivosti i dostupnosti podataka:
  * **neovlašćen pristup (čl. 2)**
  * **neovlašćeno presrijetanje podataka (čl. 3)**
  * **mijenjanje sadržaja, brisanje ili oštećenje podataka (čl. 4)**
  * **ometanja normalnog rada računara (čl. 5)**
  * **proizvodnja, prodaja, distribucije ili upotreba uređaja** projektovanih u svrhu počinjenja nekog od prethodno navedenih krivičnih djela (**čl. 6**)

# Konvencija o cyber-kriminalu

* **Zakonodavni okvir**
  * neovlašćeno korišćenje računara i računarske mreže
  * računarska sabotaža
  * pravljenje i unošenje računarskih virusa
  * računarska prevara
  * ometanje elektronske obrade i prenosa podataka i funkcionisanja računarske mreže
  * neovlašćen pristup zaštićenom računaru ili računarskoj mreži
  * sprječavanje i ograničavanje pristupa javnoj računarskoj mreži
  * neovlašćeno korišćenje autorskog i drugog srodnog prava

# Zakon o informacionoj bezbjednosti Crne Gore

* Zakon je objavljen u "Službenom listu CG", br. 113/2024 od 27.11.2024. godine, a stupio je na snagu 5.12.2024.

•Predmet zakona i
•Zakon propisuje mjere za postizanje najvišeg nivoa informacione bezbjednosti mrežnih i informacionih sistema, uključujući sajber bezbjednost, određivanje ključnih i važnih subjekata, upravljanje sajber bezbjednošću i druga pitanja od značaja za informacionu bezbjednost13.
•Obaveza primjene odnosi se na državne organe, ministarstva, lokalne samouprave, pravna lica sa javnim ovlašćenjima, privredna društva i sva druga pravna i fizička lica koja upravljaju mrežnim i informacionim sistemima

# Zakon o informacionoj bezbjednosti Crne Gore

**Definicija informacione i sajber bezbjednosti:**

- Informaciona bezbjednost podrazumijeva stanje povjerljivosti, cjelovitosti, dostupnosti i zaštite podataka, kao i sajber bezbjednost.
- Povjerljivost: podatak je dostupan samo ovlašćenim licima.
- Cjelovitost: očuvanje tačnosti i kompletnosti podataka, zaštita od neovlašćenih izmjena.
- Dostupnost: ovlašćeni korisnici mogu pristupiti podacima kad god je potrebno.

# Zakon o informacionoj bezbjednosti Crne Gore

## Zaštita od sajber prijetnji i incidenata

- Zakon propisuje mjere zaštite od sajber prijetnji i incidenata, koje obuhvataju:
  - Fizičku zaštitu objekata, prostora i uređaja gdje se nalaze mrežni i informacioni sistemi1.
  - Zaštitu mrežnih i informacionih sistema tokom obrade, skladištenja i prenosa podataka, kao i zaštitu povjerljivosti, cjelovitosti i dostupnosti podataka u svim fazama životnog ciklusa sistema1.
  - Upravljanje rizicima u oblasti sajber bezbjednosti, uključujući izradu analize rizika, pravila za postupanje sa incidentima, planove kontinuiteta poslovanja i sajber kriza, akte o bezbjednosti lanca snabdijevanja, kriptografsku zaštitu i procjenu efikasnosti mjera

# Zakon o informacionoj bezbjednosti Crne Gore

## Institucionalni okvir i nadzor

- Zaštitu mrežnih i informacionih sistema, naročito ključnih i važnih subjekata, kao i stručni nadzor nad primjenom mjera informacione bezbjednosti vrši Agencija za sajber bezbjednost.
- Vlada Crne Gore propisuje bliži sadržaj mjera informacione bezbjednosti.

## Obaveze subjekata

- Svi subjekti su dužni da imenuju odgovorno lice za praćenje primjene mjera informacione bezbjednosti.
- Obavezna je primjena mjera informacione bezbjednosti i kontinuirano praćenje njihove efikasnosti.

# Zakon o informacionoj bezbjednosti Crne Gore

## Usklađenost sa EU standardima

- Zakon je u potpunosti usklađen sa NIS2 Direktivom Evropske unije, čime Crna Gora preuzima najviše evropske standarde sajber bezbjednosti i postaje prva država Zapadnog Balkana koja ih primjenjuje.

## Posebne odredbe

- Zakon ne važi za određene državne organe iz oblasti odbrane, bezbjednosti i centralnog bankarstva, kao i za podatke čija se bezbjednost uređuje posebnim propisima o tajnosti podataka1.
- Podaci o ličnosti moraju se obrađivati u skladu sa zakonom o zaštiti podataka o ličnosti

# Copyright, patenti i licence

* **Autorsko pravo**
  * štiti originalnu implementaciju i način prikaza neke ideje, a ne samu ideju !
* **može se zaštititi izvorni i izvršni kôd**, uputstva i dokumentacija u digitalnom ili pisanom obliku.
* **ne štiti algoritme, metode i matematičke postupke** korišćene u realizaciji softvera
  * štiti od neovlašćenog kopiranja ili oponašanja koda,
  * ali ne štiti od konkurencije koja samostalno i nezavisno (bez uvida u izvorni kôd konkurencije) razvija sličan softver

# Copyright, patenti i licence

* **Patent**
* Za razliku od autorskog prava koje štiti prezentaciju ideje i oblik izražavanja, **patent štiti samu ideju**
* **Dakle, patent štiti ideje, algoritme i matematičke postupke** korišćene u programu, a ne **sam kôd**.
  * zabranjuje objavu bilo kakvog sličnog rada pa makar bio i nezavisno razvijen.
  * visoka cijena njihovog izdavanja i dugo vrijeme koje mora proći od predaje zahtjeva pa do eventualnog odobrenja za objavljivanje patenta

# Društveni aspekti sigurnosti

* **Steganografija**
  * utiskivanje jedne poruke u drugu na neki način
  * pri čemu utisnuta poruka ostaje skrivena
* **primjer – utiskivanje poruke u sliku**
  * npr za utiskivanje vlasničkih prava u sliku (watermarking)
  * **prednost u odnosu na kriptografiju: ne zna se da je poruka skrivena**

# Društveni aspekti sigurnosti

* **Sloboda izražavanja i cenzura**
* **Zabranjeni materijal** može da obuhvati lokacije sa sledećim sadržajem (shodno vladajućem režimu):
  * **materijal nepodesan za djecu i omladinu**
  * **govor mržnje** usmjeren na različite etničke, religiozne, seksualne i druge grupe
  * **informacije o demokratiji** i demokratskim vrijednostima
  * **istorijski materijali** koji protivrječe zvaničnoj verziji vlade
  * **priručnici za ilegalne aktivnosti** kao što su obijanje brava, pravljenje oružja, eksploziva i eksplozivnih naprava, razbijanje šifara i slično.

# Društveni inženjering

* **Probijanje sigurnosti iskorišćenjem ljudskog faktora**
  * nedostatka svijesti o veličini problema sigurnosti
  * nemara i grešaka
  * neobaviještenosti i neobrazovanosti

# Organizacione metode zaštite

# Analiza rizika

* Svakom projektovanju sistema zaštite treba prići s aspekta analize rizika. Tako se mogu procijeniti potrebna sredstva za njegovu realizaciju, kao i budžet neophodan za svakodnevno funkcionisanje.
* **Povrjedivost sistema** na neki događaj definiše se kao finansijski gubitak koji pretrpi neka organizacija ako se taj događaj desi.
* **Izloženost sistema** na neki događaj (rizik) definiše se kao povrjedivost na taj događaj, pomnožena vjerovatnoćom njegovog dešavanja.

# Analiza rizika

* Vjerovatnoće rizika opisuju se pomoću vremenskog intervala u kom se očekuje jedno dešavanje tog događaja. Na primer:
  * vjerovatnoća dešavanja požara je jedanput u 40 godina,
  * vjerovatnoća dešavanja operatorske greške kojom se uništava jedna datoteka je jedanput u 4 godine,
  * vjerovatnoća dešavanja softverske greške je jedanput u 10 dana.
* Ako je procijenjeno da neki događaj može da izazove gubitak od 1.000.000 €, a vjerovatnoća njegovogdešavanja za godinu dana iznosi 0,5%, onda je izloženost sistema:

$$I = P \times V = 0{,}005 \times 1.000.000 = 5.000 \text{ €}$$

# Analiza rizika

* Ukupna izloženost neke organizacije je jednaka zbiru parcijalnih izloženosti za razne događaje.
* Projektant zaštite treba da vodi računa o tome da događaje, čije istovremeno dešavanje može da dovede do narušavanja integriteta podataka, učini nezavisnim, tako da rezultantna vjerovatnoća dešavanja bude mala. Vjerovatnoće se ne mogu množiti (za dva ili više događaja) ako događaji nisu nezavisni.
* Napomenimo da se vjerovatnoća uspjeha smišljenog napada na pojedine tačke sistema ili sistem u cjelini može znatno smanjiti restrikcijom poznavanja raznih aspekata sistema – prije svega samih metoda zaštite – na one osobe koje to treba da znaju.

# Organizacione metoda

* Prilikom projektovanja i realizovanja informacionih sistema i računarskih mreža potrebno je voditi računa o skupu mjera za povećanje sigurnosti i za razumno održavanje rizika po pitanju sigurnosti na prihvatljivom nivou, uz prihvatljive troškove i uticaj na performanse sistema. Potrebno je definisati:
  * odgovornost u projektovanju tehnika i postupaka u zaštiti i
  * odgovornost za zaštitu pri svakodnevnom radu.

# Organizacione metoda

* U pogledu **odgovornosti u projektovanju tehnika i postupaka** u zaštiti neophodno je uspostaviti sledeće elemente:
  - cjelokupnu koordinaciju, odgovornost za tehnički aspekt projekta,
  - odgovornost za proceduralne kontrole,
  - odgovornost za kontrolu programa i programera,
  - odgovornost za fizičku zaštitu,
  - odgovornost za kontrolu i provjeru funkcionisanja sistema zaštite.

# Organizacione metoda

* Takođe potrebno je definisati i **odgovornost za proceduralne kontrole**:
  - operativne procedure i kontrole,
  - rad u prostoriji računara,
  - procedure i pravila kojima se štite podaci,
  - procedure potrebne kod zamjene starog sistema novim,
  - procedure koje će se primjenjivati u slučajevima otkaza računarskog sistema.

# Fizičke metode zaštite

* Domen fizičke sigurnosti sistema bavi se prijetnjema, ranjivostima i mjerama zaštite koje se mogu primijeniti kako bi se fizički zaštitili resursi i povjerljive informacije neke kompanije, orgnizacije ili institucije.
* Fizička sigurnost se najčešće odnosi na mjere koje se preduzimaju kako bi se zaštitili proizvodni i poslovni sistemi od prijetnji, kao što su provale i krađe resursa i povjerljivih informacija, pa se najjednostavnije može definisati kao proces kontrole osoblja, opreme i podataka uključenih u proces obrade informacija.

# Prijetnje fizičkoj sigurnosti

* “Velika trojka” sigurnosti (povjerljivost, integritet i raspoloživost) izložena je riziku iz fizičkog okruženja i kao takva mora biti zaštićena. Rizik predstavljaju:
  - prekidi u obezbjeđivanju računarskih usluga (raspoloživost),
  - fizičko oštećenje sistema ili pomoćne infrastrukture (raspoloživost),
  - neautorizovano razotkrivanje informacija (povjerljivost),
  - gubitak kontrole nad sistemom (integritetu),
  - krađa podataka i/ili opreme (povjerljivost, integritet i raspoloživost).

# Prijetnje fizičkoj sigurnosti

* Navodimo i nekoliko primjera prijetnji fizičkoj sigurnosti:
  - hitni slučajevi (požari i zagađenje dimom, oštećenje građevine, eksplozije, prekid snabdijevanja električnom energijom ili grijejanja, oštećenja izazvana pucanjem vodovodnih cijevi, ispuštanje toksičnih materija),
  - prirodne katastrofe (zemljotresi, klizišta, poplave),
  - ljudska intervencija (sabotaže, vandalizam, ratovi, državni udari).

# Prijetnje fizičkoj sigurnosti

* Mjere zaštite
* Jedan segment fizičke zaštite je fizička kontrola pristupa prostorijama u kojima se nalaze računari, računarska i komunikaciona oprema.
* Ovdje se mogu koristiti različite metode kontrole
  * čuvar,
  * brava sa šiframa,
  * kartične kontrole pristupa,
  * biometrijske metode.
* Tipične biometrijske karakteristike koje se mogu iskoristiti da bi se jednoznačno identifikovao identitet neke osobe su: otisak prsta, snimak mrežnjače oka, crte lica, geometrija šake, glas i svojeručni potpis.

# Kadrovski aspekti

* Prilikom izbora kadrova za rad na osjetljivim mjestima i funkcijama u okviru informacionog i komunikacionog sistema, kao i računarske mreže potrebno je voditi računa o stručnosti, povjerenju i lojalnosti.
* Za neke službe je posebna potrebna provjera u pogledu bezbjednosti, kao i rada na ranijim mjestima i uopšte stručnoj i ličnoj prošlosti kandidata.

# Kadrovski aspekti

* Pri svakodnevnom radu, poseban značaj u pogledu odgovornost za zaštitu pri svakodnevnom radu imaju:
  - Rukovodilac računarskog centra - Zadužen je za raspodjelu odgovornosti u oblasti zaštite i ima odgovornost za striktnu i neprekidnu primjenu mjera zaštite.
  - Administrator zaštite.
  - Lokalni službenici zaštite.
  - Vlasnici datoteka.
  - Kontrolori zaštite.

# Sigurnosna politika preduzeća

* Pitanje sigurnosti je veoma bitno u eri koju karakteriše kompleksno računarsko okruženje, sa mnogim računarskim platformama i sa ogromnim konglomeratom integrisanih računarskih mreža. Implementacija sistem sigurnosti na nivou preduzeća, institucije ili organizacije je često vrlo komplikovan i nedovoljno definisan zadatak.
* Ovom prilikom je potrebno razmotriti određena pitanja, kao što su na primjer:
  - Koliki je stepen sigurnosti neophodan i koje vrste sigurnosti najefektnije zadovoljavaju konkretne zahtjeve kao poslovnog subjekta?
  - Odakle početi u definisanju i postavljanju sistema sigurnosti?
  - Kako korisnik informacione tehnologije možete ostvariti i održati ekonomičan nivo sigurnnosti informacionog sistema sa prihvatljivom cijenom (troškom).

# Sigurnosna politika preduzeća -
## Sigurnosna odgovornost

* Politika sigurnosti IT mora jasno i nedvosmisleno ukazivati ko je odgovoran za sigurnost.
* U pojednostavljenom smislu značenja “svi” su odgovorni znači i "niko".
* Politika sigurnosti mora zahtijevati od svih korisnika da potpišu ugovor, koji jasno određuje njihovu specifičnu sigurnosnu odgovornost i potrebno znanje koje bi trebalo da u sebi sadrži elemente poznavanja sistema i podataka. Sledeće tačke moraju biti pokrivene u ugovoru:
  - organizacija je vlasnik sistema IT i podataka,
  - korisnik se slaže da nije i da neće učiniti neautorizovane kopije podataka i softvera,
  - korisnik se slaže da izabere sigurnosnu šifru (password) na promišljen način

  te da će je držati i očuvati tajnom,
  - korisnik se slaže da pristupi sistemu i podacima samo na autorizovan način,
  - Korisnik poznaje prava organizacije praćenja sistema za sigurnosne svrhe.