UDC: 007:004.056 INFO M: str. 13-16

INFORMACIONA BEZBEDNOST I RANJIVOST "PAMETNIH" ELEKTROENERGETSKIH MREŽA CYBER SECURITY AND VULNERABILITY OF „SMART" POWER GRIDS

Slobodan Jovanović
Univerzitet Metropolitan, Fakultet informacionih tehnologija, Beograd, www.metropolitan.edu.rs,

REZIME: Pametna mreža isporučuje energiju od proizvodjača do potrošača koristeći two-way Smart Meter technology (pametna brojila), koja može daljinski da kontroliše upotrebu energije korisnika. Medjutim, ove mreže postaju sve više i više vrlo atraktivni ciljevi hakera i terorista. Ovaj rad diskutuje ključne karakteristike informacione bezbednosti i informacione ranjivosti „pametnih" elektroenergetskih mreža, kao i njihovu komunikacionu arhitekturu, i njihove tačke ranjivosti. Zatim, opisuje direktive koje je potrebno primeniti da bi se postigla informaciona bezbednost tj. minimizirala informaciona ranjivost u „pametnim" elektroenergetskim mrežama, i dotiče pitanje razvoja njihovih informacionih bezbednosnih standarda. Takodje, prikazuje se plan za razvoj informacione infrastrukture „pametnih" elektroenergetskih mreža u EPS (Elektroprivredno preduzeće Srbije) za sledećih 10 godina.

KLJUČNE REČI: Informaciona infrastruktura, Logički interfejs, Distribuirana inteligencija, Distribuirani generatori

ABSTRACT:Smart power grids deliver electric energy from generation to consumers using two-way Smart Meter technology (smart meters), enabling remote control of consumer energy use. However, smart power grids are increasingly very attractive targets for hackers and terorists. This paper discusses the key characteristics of cyber security/vulnerability of smart power grids, and their communication architecture, and their vulnerability points. Then, it describes guidelines which are needed to be implemented to achieve cyber security and minimise cyber vulnerability in smart power grids, and a question of development of their cyber security standards. Finally, the plan for development of information infrastructure of smart power grids in Serbia (EPS – Electris power of Serbia) in next 10 years is presnted here..

KEY WORDS: Information infrastructure, Logical interface, Distributed intelligence, Didtributed generation

1. UVOD

Od početka 21-og veka, poboljšanje i pojeftinjenje komunikacionih tehnologija pružili su mogućnost da se unapredi upravljanje elektroenergetskim sistemima tj. elektroenergetskim mrežama. Vetrogeneratori i sunčevi generatori (*wind power , solar power*) imaju veoma promenljivu izlaznu snagu, pa je sofisticiranije tj. „inteligentno" upravljanje ovim izvorima neophodno. Digitalne komunikacije i digitalno procesiranje i distribuirana inteligencija su osnovne osobine „pametne" elektroenergetske mreže. Pametna brojila (*smart meters*) su digitalna brojila koja čitaju i memorišu u realnom vremenu, i koja mogu da isključe pojedine potrošače u vreme maksimalnih tj. kritičnih opterećenja sistema.

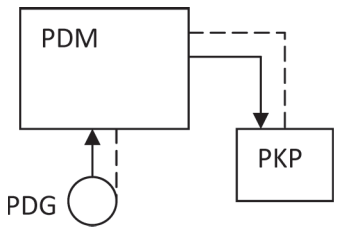
Elektroenergetska mreža koja radi blizu svojih limita tj. blizu svog maksimalnog kapaciteta, zahteva sve više i više primenu „pametnih" tehnologija. Naime, buduće distributivne mreže radiće u uslovima gde se koristi veliki procenat DG (*distributed generation, tj. embeded generation*), a DG može da ima veoma varijabilnu i nepredvidljivu izlaznu snagu. Takodje, energija postaje sve skuplja, i ide se na minimizaciju učešća fosilnih izvora energije, i uopšte na minimalnu potrošnju energije. Dakle, distributivne mreže budućnosti radiće sa velikim učešćem DG, i sve više se nameće potreba za „pametnim" mrežama **[1],** gde se omogućuje primena

- Distribuirane inteligencije
- Digitalne komunikacije
- Softvera za upravljanje

Digitalne dvosmerne komunikacije, tj. *two-way fast digital communications*, mogu biti različitog tipa:

- Fiksni i bežični telefoni
- Radio veza
- Optički kablovi
- Energetski vod (*power line carrier*)
- Satelit
- Intenet

Na slici 1 je prikazana „pametna" distributivna mreža PDM tj. tzv. *„smart" power grid SPG*. „Pametni" krajnji potrošač PKP i „pametni" distribuirani generatori PDG su ključni elementi u okviru PDM. Pri tome, distribuirana inteligencija je deo PKP i PDG. Dakle, PDM i PDG se „inteligentno" ponašaju tj. prilagodjavaju uslovima rada u sistemu, u cilju što efikasnije i bezbednije upotrebe PDM.



Slika 1: Pametna disdtributivna mreža PDM
(isprekidana linija predstavlja komunikacioni kanal)

Smart grid je kišobran koji pokriva modernizaciju kako distributivne tako i prenosne elektroenergetske mreže. Kod

prenosne meže, umesto upravljanja malim generatorima DG i krajnjim potrošačima KP, cilj je primena „pametnih“ tehnologija na upravljanje elementima u prenosnom sistemu.

Tradicionalni SCADA sistemi predstavljaju u stvari začetak „pametnih“ elektroenergetskih mreža. Tj. SCADA je najranija *smart grid* tehnologija. Ipak, tradicionalna SCADA doseže samo do podstanica (i to ne svih), glavnih vodova, i malog broja daljinsko-kontrolisanih uredjaja (npr. rastavljača). Pošto je u distributivnoj mreži DM broj vodova i čvornih tačaka ogroman, a kapitalni troškovi (investicije) za RTU su veliki (RTU su vrlo skupe), onda je i broj RTU limitiran u tradicionalnoj distributivnoj mreži. SCADA i podaci u okviru SCADA sistema igraju važnu ulogu u bilo kojoj implementaciji „pametne“ elektroenergetske mreže.

2. RANJIVOST „PAMETNIH“ MREŽA

Pametna mreža isporučuje energiju od proizvodjača do potrošača koristeći *two-way Smart Meter technology* (pametna brojila), koja može daljinski da kontroliše upotrebu energije korisnika. Ovo omogućuje konzervaciju energije, redukovane troškove, veću pouzdanost i efikasnost. Ali, takvi IT-bazirani elektroenergetski sistemi dramatično povećavaju ranjivost informacione bezbednosti (*cyber security vulnerabilities*), i ovo dovodi do dramatično povećanog značaja informacione bezbednosti **[2,3,4].**

U današnjoj (tradicionalnoj) elektroenergetskoj mreži, puno komunikacije se sprovodi pomoću telefona. Medjutim, protok podataka postao je vrlo važan za jednu elektroenergetsku mrežu. Npr. raspad sistema od 14.8.2003. u USA je bio uzrokovan kašnjenjem u komunikaciji uzbune u sistemu. Takodje, mnogi drugi ispadi u sistemu su rezultat kašnjenja ili greške u informaciji. Takodje, dolazi do kvarova u IT infrastrukturi, koji nisu rezultat terorističkog ili hakerskog napada. Tako da informaciona bezbednost treba da se bavi ne samo namernim napadima na sistem, već i kvarovima u IT infrastrukturi i protoku informacija.

Širom sveta, elektroprivredne organizacije i vlade tih država rade na izgradnji pametnih elektroenergetskih mreža. Medjutim, ove mreže postaju sve više i više vrlo atraktivni ciljevi hakera i terorista. U najnovijim istraživanjima u tom polju, elektroenergetska mreža neke zemlje je identifikovana medju tri najvažnija i najranjivija cilja hakera i terorista, zajedno sa telekomunikacionom nacionalnom mrežom i IT infrastrukturom nacinalne odbrane i bezbednosti (vojska).

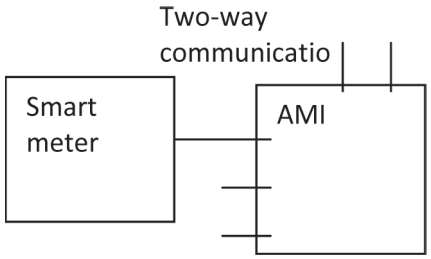
Pametne EE (elektroenergetske) mreže obuhvataju IT infrastrukturu koja je mnogo više integrisana sa EE mrežom, i ovo dramatično povećava ranjivost EE mreže na napade na informacionu bezbednost. Broj tačaka koje mogu biti napadnute (*threat surface*) dramatično se uvećava kada se od sadašnje mreže pomerite u pametnu EE mrežu. Naime, u jednoj pametnoj EE mreži, IT infrastruktura se proteže od „tostera do turbine„ sa ujedinjenom kontrolom mreže, pa zato napadi mogu da se prošire mnogo lakše i i ima mnogo više tačaka za napad **[4].** Naime, milioni i milioni potrošača sa svojim pametnim brojilima i kućnim HAN (*Home Area Network*) mrežama postaju potencijalne tačke napada.

U USA postoje izveštaji da hakeri i teroristi pokušavaju da napadnu EE mrežu. I u drugim zemljama, ranjivost pametne EE mreže postaje sve veći i veći problem. Kao rezultat, sve veća i veća novčana sredstva se izdvajaju da bi se ovaj problem uspešno rešio. Dakle, u narednom periodu, velike investicije će biti angažovane da bi se rešavao problem informacione ranjivosti (*cyber security vulnerabilit*y) pametnih EE mreža. Procenjuje se da će oko 15% od totalnih investicija u pametne EE mreže ići na informacionu bezbednost, što su ogroma sredstva. Npr. u 2015. procenjuje se da u USA ova sredstva će iznosti oko 1.5 milijardu dolara **[4].**

Prema tome, EE mreža se modernizuje i transformiše u pametnu mrežu, uključivanjem IT infrastrukture i tehnologija, ali elektroprivredne organizacije i vlade država su shvatile da se ne može imati pametna EE mreža bez „pametne bezbednosti“ („*smart security*“). Opasnost od napada na informacionu bezbednost nije više imaginarna i teorijska već vrlo realna i prisutna, i sve veća **[2].**

Konvencionalna brojila su elektroemehanička, ali njihova funkcionalnost nije adekvatna za pametne mreže. Pametno brojilo (*smart meter*) je u stvari elektronsko brojilo kje ima i memoriju, softver, i telekomunikacioni kanal. Pametno brojilo je u stvari jedan mali računar sa kojeg se mogu učitavati podaci iz daljine, i koje se može kontrolisati iz daljine (*read and managed remotely*). Pametno brojilo predstavlja jedan telekomunikacioni čvor integrisan u telekomunikacionu mrežu, gde se vrši učitavanje kWh i upravlja brojilom i potrošačem (pogledati sliku 2).

Pomoću pametnog brojila može se vršiti učitavanje kWh iz daljine i automatski i napraviti račun za potrošnju el. energije (nije potrebno manuelno učitavanje na licu mesta od strane fizičkog lica), mogu se isključiti potrošači iz daljine kada je to potrebno, i ponovo uključiti, daljinske promene tarife, individualne tarife, itd.



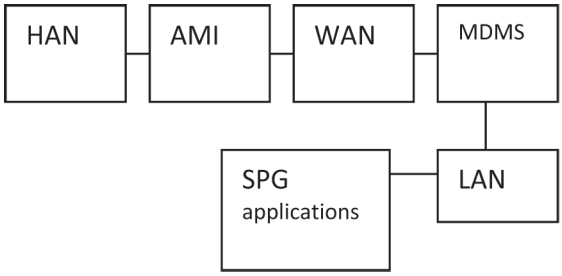
Slika 2: Pametno brojilo u sebi sadrži elektronsko merenje, memoriju i softver, i koje se može čitati i dirigovati iz daljine

Medjutim svako pametno brojilo je i tačka informacione ranjivosti pametne mreže. U Španiji se planira do kraja 2018 g. da bude instalisano 30 miliona pametnih brojila. Ali, svako ovo brojilo je i tačka mogućeg napada na informacionu bezbednost pametne mreže.

3. KOMUNIKACIONA ARHITEKTURA I TAČKE RANJIVOSTI

Advanced Metering Infrastructure (AMI) i *Meter Data Management System* (MDMS) su osnovne komponente komunikacione arhitekture pametne elektroenergetske mreže. AMI prikuplja i transmituje *Smart Meter data*, a MDMS prikuplja,

memoriše i operiše ovim podacima **[2].** Na slici 3 je prikazana komunikaciona arhitektura pametne mreže, koja obuhvata HAN (*Home Area Network*), AMI komunikacionu mežu i WAN (Wide Area Network), i MDMS.



Slika 3: Komunikaciona arhitektura pametne mreže (*smart power grid* - SPG)

Sa razvojem MDMS tehnologije, MDMS podaci se koriste za novije aplikacije, uključujući aplikacije za

- Web portale potrošača,
- interne Web portale,
- *independents system operators* ISO,
- i proizvodjače energije

Ovo omogućuju efikasnije upravljanje sistemom, a potrošačima energije pružaju bolje informacije o njihovoj potrošnji.

Ali, ovde se pojavljuju novi rizici. Naime, kako elektroprivredne kompanije primenjuju savršenije tehnologije i dodaju inteligenciju elektroenergetskoj mreži, ove nove tehnologije donose nove tačke ranjivosti u pametnu mrežu (komunikacioni protokoli, logički interfejsi, HAN, *customer portals*, hardver) **[2]:**

1) Npr. **komunikacioni protokoli** kod komunikacija izmedju AMI aparata i MDMS, i ova komunikacija može biti ugrožena ako komunikacija nije šifrovana od početka do kraja (*encrypted end-to-end*). Naime, autentifikacija i autorizacija izmedju aparata treba da se šifruje.
2) **Logički interfejsi** pametne mreže, kao što su Web-bazirane aplikacije, su predmet ranjivosti u vezi sa protokolima i aplikacijama koje se koriste u pametnoj mreži.
3) **HAN** tj. aparati u okviru HAN su takodje tačka ranjivosti. Pri tome, bežična komunikacija izmedju pametnih aparata i centralnog sistema treba da se zaštiti protiv napada.
4) Napadači na pametnu mrežu mogu da koriste ***customer portals*** da pristupe računima potrošača i promene podešenja tj. podatke o potrošačima. I ovo može da utiče na mrežu a i potrošače.
5) **Hardver** takodje donosi tačke ranjivosti. Naime, pametno brojilo (Smart Meter) je povezan sa AMI, i ovo donosi rizik sličan sa rizikom od bežičnog HAN. Neka neautorizovana osoba mogla bi da kontroliše brojilo, da ga uključi ili isključi ili modifikuje podešenje. Ovo ima posledice za potrošača a i za proizvodjača energije.

4. DIREKTIVE ZA INFORMACIONU BEZBEDNOST I RANJIVOST

U celom svetu, a najviše u USA, je započela velika transformacija infrastrukture elektroenergetskih mreža. Ova ogromna nadogradnja infrastrukture se dešava u svim delovima, od domaćinstava do velikih elektrana, i do vetrofarmi i DG. Ova promena je istovremeno i evolutivna i revolucionarna. U USA je CSWG grupa (Cyber Security Working Group) zadužena da daje direktive, i ona je objavila dokument „*Guidelines for Smart Grid Cyber Security*“ **[3].** Ovaj dokument se koristi u mnogim organizacijama da one razviju efektivne strategije za informacionu bezbednost, i to za njihovu konkretnu kombinaciju *smart-grid* karakteristika i konvencionalne mreže. *Smart-grid* je koncept, a ne unificirana kombinacija hardvera. Elktroenergetski sistemi se dramatično menjaju poslednjih godina, i ovo će potrajati još niz godina, i opasnost od napada na informacionu bezbednost EE mreža je veliki **[4].**

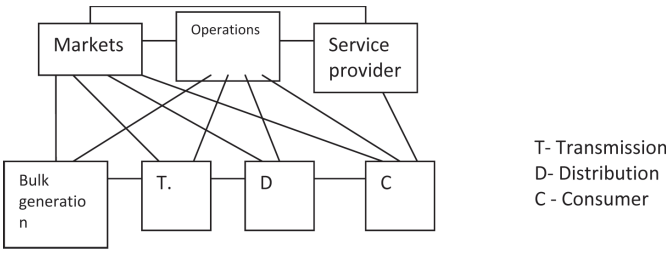
Može se definisati 7 informacionih domena u jednoj pametnoj prenosno-distributivnoj mreži: Prenos, Distribucija, Operacije (tj. Upravljanje), Velike elektrane, Tržišta, Potrošači, Servis provajder **[3].** Ovih 7 domena je povezano tokovima informacija, kao što se vidi na slici 4. Ovih 7 domena sadrže 46 poddomena tj. aktera. Npr. ISO operatori (*Independent system operator*) su prisutni kako u domenu Operacije tako i u domenu Tržišta.

Takodje, identifikovano je 130 mogućih tipova logičkih interfejsa. I ovih 130 tipova interfejsa se može razvrstati u 22 kategorije. Za svaki od ovih interfejsa, može se proceniti uticaj nenamernog ispada ili namernog napada na ovaj interfejs.

S obzirom na mnogo raznih interfejsa, da treba posmatrati bezbednost u nekoliko slojeva. Npr.

- *loss of confidentiality* (razotkrivanje informacije)
- *loss of integrity* (modifikacija/destrukcija informacije)
- *loss of availability* (gubitak pristupa informaciji)

Preko analize domena, aktera, i komunikacionih zahteva, u pametnoj mreži, mogu se razvrstati logički interfejsi u razne kategorije.



Slika 4: Informacioni domeni „pametne“ prenosno-distributivne mreže i tokovi komunikacija (7 domena i 15 tokova informacija)

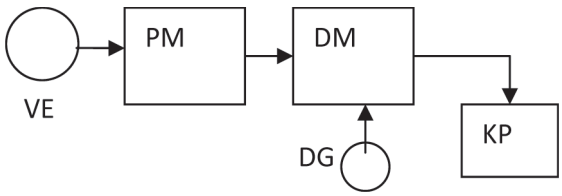
IEC TC57 je familija internacionalnih standarda za pametne mreže, uključujući IEC61850. Na osnovu USA *Energy Independence and Security Act* iz 2007., NIST (*National Institute of Standards nd Technology*) je zadužena za identifikaciju i selekciju stotine standarda koji će biti potrebni da se implementiraju u *Smart Grids* u Americi (USA). Ovi standardi će se podneti kod FERC (*Federal Energy Regulatory Comission*). Ovaj rad na standardima tj. njihovom razvoju, je započet, i prvi standardi su već izabrani.

Sada postoji trend da se koriste TCP/IP tehnologije kao zajedničke komunikacione platforme za primenu pametnih brojila, tako da elektroprivredne organizacije mogu da primene različite komunikacione sisteme, ali korišćenjem IP tehnologije kao zajedničke platforme.

U Wikipediji može se naći opis TCP/IP **[5]:** "The **Transmission Control Protocol** (**TCP**) is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite, complementing the Internet Protocol (IP), and therefore the entire suite is commonly referred to as *TCP/IP*. TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. TCP is the protocol used by major Internet applications such as the World Wide Web, email, remote administration and file transfer. "

5. RAZVOJ *SMART GRID* U EPS

Postoje dve vrste elektroenergetskih mreža, prenosne i distributivne mreže. Prenosna mreža (PM) koristi napone od 110 kv pa na više (110 kV, 220kV i 400kV), dok distributivna mreža (DM) koristi napone srednjeg nivoa (10 kV, 20kV, itd) i niskog nivoa (220 V, 400V). Distributivna mreža je veza izmedju prenosne mreže i krajnjih potrošača KP, dok je prenosna mreža veza izmedju velikih elektrana (VE) i distributivne meže, kao što je prikazano na slici 5. Male elektrane tj. tzv. distribuirani generatori (DG) su priključeni na distributivnu mrežu. DG se često definiše kao proizvodnja locirana kod potrošača (neki potrošači proizvode el. energiju koristeći sopstvene generatore, npr. od 1kW ili npr. 100 kW). Distributivni sistem obuhvata DM (distributivna mreža), DG i KP, ali DM takodje obuhvata HV/MV i MV/LV trafostanice TS, MV i LV vodove (glavne i sporedne vodove, *feeders/subfeeders*), kao i MV i LV čvorne tačke (MV i LV podstanice) **[6].**



Slika 5: Prenosna i distributivna elektroenergetska mreža

U EPS postoji plan za implementaciju projekta „EPS *Metering*" **[7].** U EPS ima oko 3.5 miliona potrošača, od kojih oko 3.1 milion domaćinstava. Postoji plan da u roku od 10 godina se preuzmu merna mesta od kupaca. I uspostavljanje AMI-MDM sistema. U fazi 1 zamena merne infrastrukture kod velikih potrošača i uvodjenje kontrolnih mernih mesta u TS x/0.4 kV. Po završetku prve faze, planira se verifikacija funkcionalnosti AMI-MDM sistema. U fazi 2a, zamena 50.000 mernih uredjaja u domaćinstvima i instalacijom 3.000 AMI koncentratora. U fazi 2b, zamena 300.000 menih uredjaja u domaćinstvima i ugradnjom 5.000 AMI koncentratora. Po završetku faze 2, masovna ugradnja kod ostalih potrošača a gde je to ekonomski opravdano, oko 80%, u roku od 7 godina. Faza 3 obuhvata zamenu oko 2.2 miliona mernih uredjaja domaćinstava, i ugradnjom potrebnog broja koncentratora.

Faza 1 trajaće oko 1.5 godina, faza 2a oko 1 godine, faza 2b oko 2.5 godine, i faza 3 oko 7 godina. Ukupno trajanje projekta je oko 10 godina. Tabela 1 sumarizuje razvoj pametne distributivne mreže u EPS. Prenosna mreža Srbije EMS, je posebna organizacija koja je izvan EPS.

Tabela 1: Razvoj pametne distributivne mreže u EPS

Faza	Broj instalisanih *smart-meters*
1	Veliki potrošači i TS x/0.4
2a	50.000 domaćinstava
2b	300.000 domaćinstava
3	2.250.000 domaćinstava

U EPS-u se planiraju značajne investicije u obnovljive izvore enegije OIE u sledećih 10 godina. Npr. u 2012. g. plan razvoja OIE u JP EPS je sledeći:

- nastavak ulaganja sa stranim partnerima u Moravske hidroelektrane (HE) i Ibarske HE
- izgradnja solarne elektrane na Zlatiboru od 5 MW
- izgradnja termoelektrane-toplane u Sremskoj Mitrovici, koja koristi kao gorivo ljuspice suncokreta
- izgradnja solarnih panela na objektima EPS-a
- ugovaranje izgradnje 8 novih malih HE, ukupne snage 14 MW
- revitalizacija postojećih malih HE, ukupne snage od 17 MW

6. ZAKLJUČAK

Ovaj rad diskutuje neke ključne karakteristike informacione bezbednosti i ranjivosti „pametnih" elektroenergetskih mreža, i pri tome razmatra njihovu komunikacionu arhitekturu, kao i njihove tačke ranjivosti. Rad specificira direktive koje je potrebno primeniti da bi se postigla informaciona bezbednost tj. minimizirala ranjivost u „pametnim" elektroenergetskim mrežama, kao što i dotiče pitanje razvoja informacionih bezbednosnih standarda „pametnih" mreža. Takodje, definišu se informacioni domeni u prenosno-distributivnoj „pametnoj" elektroenergetskoj mrežii, i tokovi informacija medju ovim domenima. Konačno, prikazuje se plan za razvoj informacione infrastrukture „pametnih" distributivnih elektroenergetskih mreža u Srbiji tj. u EPS (Elektroprivredno preduzeće Srbije) za sledećih 10 godina.

ZAHVALNICA

Ovaj rad podržan je od strane Ministarstva za nauku i obrazovanje (Projekat III44006).

LITERATURA

[1] A.Sellim, O.Malik, Electric distribution systems, Wiley, 2011.
[2] KPMG, The increasing importance of security for the smart grid, www.kpmg.com .
[3] Cyber Security Working Group (CSWG)., *Guidelines for Smart Grid Cyber Security*, http://nist.gov./smartgrid/ .
[4] M.Stevens, „Smart" power grids a prime target in cyber warfare, http://www.securityweek.com/smart-power-grids-prime-target-cyber-warfare
[5] http://en.wikipedia.org/wiki/TCP/IP
[6] T. Flick, J.Morehouse, Securing the Smart Grid – Next Generation Power Grid Security, Elsevier - Syngress, 2011.
[7] Javno Preduzeće EPS, Plan za implementaciju projekta „EPS METERING", mart 2012.

Slobodan Jovanović, Prof. Dr. Inž., predaje na Univerzitetu Metropolitan, Fakultetu za informacione tehnologije
slobodan.jovanovic@fit.edu.rs