



Prevenција je stvar ZNANJA, INTELEKTA, SAZREVANJA i ISKUSTVA – ZITEH '10

Uputstvo za autore radova na savetovanju ZITEH '10

Autorski radovi bi trebalo da sadrže uobičajena poglavlja: naslov, ime i prezime autora, naziv i adresa ustanove u kojoj je rad izrađen, elektronska adresa autora (ukoliko je ima), kratak izvod (abstrakt) na srpskom i engleskom, koji ne bi trebalo da bude duži od 150 reči, odnosno 10 redova, listu od 4 do 6 ključnih reči, uvod, razradu, zaključak i popis korišćene literature.

Rukopis pripremiti u nekoj verziji Worda, korišćenjem fonta Times New Roman, veličina slova 12 pointa, na formatu A4 i marginama od 2,5 cm, izuzev leve koja treba da je 3 cm. Veličina rada ne bi trebalo da bude veća od 1 autorskog tabaka (16 strana).

Tabele, šeme, grafikoni i slike trebalo bi da budu jasni i pregledni i ugrađeni u dokument.

Numerisan popis literature se abecedno uređuje po prezimenu autora i početnom slovu imena. Pored toga, navode se uobičajeni bibliografski podaci. Za knjigu se navodi naziv knjige, naziv izdavača, mesto i godina izdavanja. Za časopis se navodi naslov članka, naziv časopisa, broj i godinu izdanja, i strane od – do u časopisu. Za materijale sa Interneta treba navoditi i njihove Internet adrese. Nazivi knjiga i članaka se navode u originalu.

Prispeli radovi podležu ***uređivačkoj obradi i anonimnoj recenziji.***

Rukopise u elektronskoj formi na CD-u, sa naznakom za savetovanje ZITEH '10 slati na adresu: IT VEŠTAK, Danijelova 32, 11.000 Beograd

Radovi se takođe mogu poslati i elektronskom poštom na adresu: **itvestak@ptt.rs**

Rok za dostavu rukopisa je 25. februara 2010. godine

Beograd, 24.12.2009. god.

Tehnički sekretar
Živko Dženopoljac

Predsednik Organizacionog odbora
Vesna Pajković Pudar, dipl. ing. el.

Okvirne teme savetovanja ZITEH '10

ZLOUPOTREBE IT

- Krimogeni faktori
- Potencijalni ciljevi zloupotrebe
- Kategorije zloupotrebe
 - Kompjuterski kriminal
 - Kiber-terorizam
 - Obaveštajno delovanje
 - Informaciono ratovanje
- Nove forme zloupotreba IKT
- Metode i tehnike zloupotrebe
- Motivi i profili izvršilaca
- Otkrivanje i dokazivanje
- Mesto i uloga državnih organa, obrazovnih ustavona i medija
- Sudsko veštačenje u oblasti IKT
- Sankcionisanje
- Terminologija i standardi
- Informatička etika
- Međunarodna saradnja u oblasti kompjuterskog kriminala
- Forenzički alati
 - Hardverski alati
 - Softverski alati
 - Verifikacija i validacija alata
- Digitalna forenzika (računara, RM, softvera)
- Digitalna forenzika računara u radu (*live forensic*)
- Forenzičke tehnike i alati za upravljanje kompjuterskim incidentom

ZAŠTITA

- Informaciona bezbednost
- Politike zaštite
- Arhitektura sistema zaštite
- Aspekti zaštite:
 - Normativni aspekt
 - Fizičko-tehnički aspekt
 - Logički aspekt
- Kripto zaštita
- KEMZ i zaštita
- TEMPEST standard i zaštita
- Steganografija i Digitalni vodeni pečat
- Zaštita baza podataka
- Zaštita personalnih računara
- Zaštita u računarima i računarskim mrežama
- Zaštita na Internetu
- Metodologija zaštite web aplikacija
- Zaštita intelektualne svojine
- Zaštita privatnosti
- Evoluacija sistema zaštite (sertifikacija i akreditacija)
- Metrički sistemi u oblasti zaštite
- Upravljanje rizikom (modeli i metodi)
- Upravljanje programom zaštite
- Dokumenta i standardi zaštite
- Metodologije za razvoj sistema zaštite
- Projektovanje sistema zaštite
- Etičko hakovanje
- Evaluacija i poboljšavanja procesa zaštite
- Zakonska regulativa u svetu i kod nas
- Modeli obuke