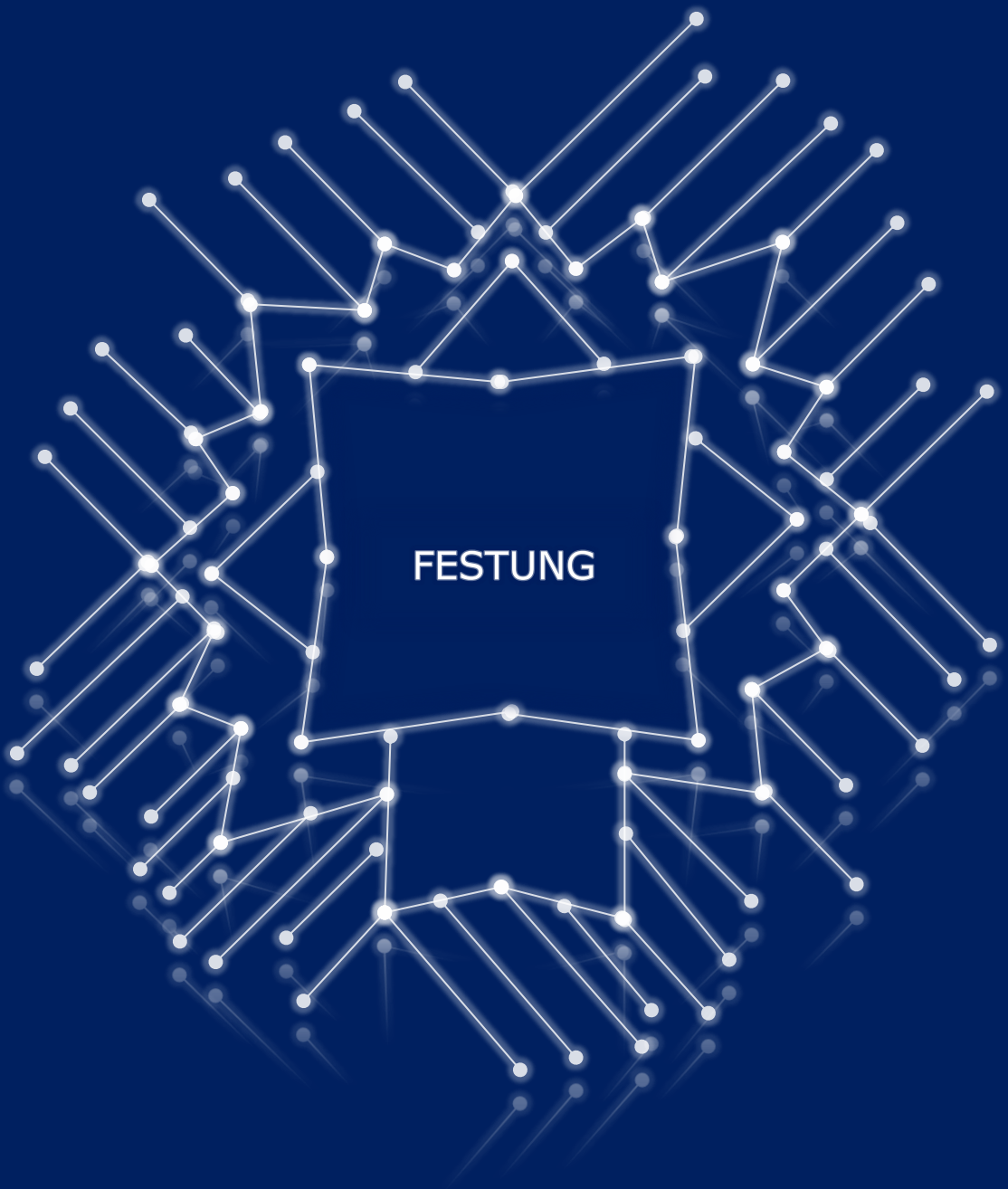
Znanstveno – stručna konferencija

FESTUNG

Slavonski Brod

11. do 13. lipnja 2025. godine



Sveučilište u Slavonskom Brodu

Knjižica sažetaka

Slavonski Brod, 2025. godine

CYBER FESTUNG

SVEUČILIŠTE U SLAVONSKOM BRODU

Trg I. B. Mažuranić 2
35000 Slavonski Brod

tel: +385 35 446 188
https://festung.unisb.hr/

OIB: 3302783437
IBAN:HR0923400091111084627

Knjižica sažetaka Festung proizašla je iz aktivnosti projekta Cyber Festung

Projekt FSTP-OI-22: Cyber Festung Sveučilišta u Slavonskom Brodu ima za cilj povećati svijest o kibernetičkoj sigurnosti među građanima i organizacijama. Kroz istraživanje, analize, edukaciju, simulacije i druge aktivnosti, projekt će jačati otpornost na cyber napade. Ciljne skupine su zaposlenici, studenti, učenici i poslodavci. Očekivani rezultati su bolja zaštita podataka, povećana svijest o rizicima i jača suradnja između različitih dionika u području kibernetičke sigurnosti.

Stopa sufinanciranja ovog projekta iznosi 100% ukupnih prihvatljivih troškova projekta navedenih u sklopu projektne prijave. 50% ukupnih prihvatljivih troškova podmiruje Europska unija, 50% Erste banka.

https://festung.unisb.hr/

ERSTE Bank | Cyber Guardian

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

CYBER FESTUNG

SVEUČILIŠTE U SLAVONSKOM BRODU

Trg I. B. Mažuranić 2

35000 Slavonski Brod

tel: +385 35 446 188

https://festung.unisb.hr/

OIB: 3302783437

IBAN:HR0923400091111084627

Znanstveno – stručna konferencija

FESTUNG

Slavonski Brod

11. do 13. lipnja 2025. godine

KNJIŽICA SAŽETAKA

Slavonski Brod, 2025. godine

ERSTE Bank | Cyber Guardian

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

Organizator konferencije

Sveučilište u Slavonskom Brodu

Izdavač

Sveučilište u Slavonskom Brodu

Za izdavača

prof. dr. sc. Ivan Samardžić

Glavni urednik

doc. dr. sc. Mirko Cobović

Urednici

doc. dr. sc. Maja Vretenar Cobović

doc. dr. sc. Sanela Ravlić

prof. dr. sc. Antun Stoić

Lektura i korektura

dr. sc. Željka Rosandić

doc. dr. sc. Irena Krumes

Oprema i prijelom

doc. dr. sc. Mirko Cobović

Naklada

Knjižica je dostupna u elektroničkom izdanju i nalazi se na mrežnim mjestima: Znanstveno – stručna konferencija Festung i službenim stranicama Sveučilišta u Slavonskom Brodu

ISBN:978-953-8426-05-6

Slavonski Brod, 2025. godine

Programski odbor

doc. dr. sc. Maja Vretenar Cobović, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Mirko Cobović, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Sanela Ravlić, Sveučilište u Slavonskom Brodu, Hrvatska

prof. dr. sc. Antun Stoić, Sveučilište u Slavonskom Brodu, Hrvatska

prof. dr. sc. Branimir Dukić, Ekonomski fakultet u Osijeku, Hrvatska

prof. dr. sc. Mislav Šimunić, Fakultet za menadžment u turizmu i ugostiteljstvo, Sveučilište u Rijeci, Hrvatska

prof. dr. sc. Jerko Glavaš, Ekonomski fakultet u Osijeku, Hrvatska

prof. dr. sc. Marinko Stojkov, Sveučilište u Slavonskom Brodu, Hrvatska

prof. dr. sc. Roberto Lujić, Sveučilište u Slavonskom Brodu, Hrvatska

prof. dr. sc. Dražan Kozak, Sveučilište u Slavonskom Brodu, Hrvatska

izv. prof. dr. sc. Tomislav Matić, Fakultet elektrotehnike, računalstva i informacijskih tehnologija, Hrvatska

izv. prof. dr. sc. Zdravko Krpić, Fakultet elektrotehnike, računalstva i informacijskih tehnologija, Hrvatska

izv. prof. dr. sc. Ivan Aleksi, Fakultet elektrotehnike, računalstva i informacijskih tehnologija, Hrvatska

izv. prof. dr. sc. Nikola Papac, Ekonomski fakultet Mostar, Bosna i Hercegovina

izv. prof. dr. sc. Várady Géza, University of Pécs, Mađarska

izv. prof. dr. sc. Željko Vojinović, Ekonomski fakultet Subotica, Srbija

izv. prof. dr. sc. Bojan Leković, Ekonomski fakultet Subotica, Srbija

izv. prof. dr. sc. Tomislav Jakopec, Filozofski fakultet Osijek, Hrvatska

doc. dr. sc. Hrvoje Serdarušić, Ekonomski fakultet u Osijeku, Hrvatska

Organizacijski odbor

doc. dr. sc. Maja Vretenar Cobović, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Mirko Cobović, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Sanela Ravlić, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Anita Kulaš Mirosavljević, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Lena Sigurnjak, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Sanja Knežević Kušljić, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Ivana Miklošević, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Milan Stanić, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Višnja Bartolović, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Andreja Katolik Kovačević, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Ivona Blažević Dević, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Hrvoje Sivrić, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Matej Galić, Veleučilište Lavoslav Ružička u Vukovaru, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Zrinka Šimunović, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Matilda Kolić Stanić, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Irena Krumes, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Katarina Šarčević Ivić-Hofman, Sveučilište u Slavonskom Brodu, Hrvatska

doc. dr. sc. Tomislav Alinjak, Hrvatska elektroprivreda, Hrvatska

doc. dr. sc. Sara Havrlišan, Sveučilište u Slavonskom Brodu, Hrvatska

dr. sc. Željka Rosandić, Sveučilište u Slavonskom Brodu, Hrvatska

dr. sc. Ivana Unukić, Ekonomski fakultet u Osijeku, Hrvatska

dr. sc. Antun Barac, Sveučilište u Slavonskom Brodu, Hrvatska

Ivan Stipić, knjiž. savjetnik, Sveučilište u Slavonskom Brodu, Hrvatska

Maja Čuletić Čondrić. prof., v. pred., Sveučilište u Slavonskom Brodu, Hrvatska

Marija Stoić, mag. ing. stroj., v. pred., Sveučilište u Slavonskom Brodu, Hrvatska

Marina Stanić Šulentić, univ. mag. oec., Sveučilište u Slavonskom Brodu, Hrvatska

Mato Kokanović, mag. ing. el., pred.

Ivan Matasović, mag. inf. el., pred.

Zdravko Janeš, dipl. oec., pred.

Ivan Marušić, dipl. ing. el., pred.

Tin Horvatin, mag. oec., asist.

Krešimir Herceg, dipl. oec., asist.

Miroslav Mazurek, dipl. ing. el.

Damir Lulić

Predgovor

Poštovani sudionici i cijenjeni čitatelji,

s iznimnim zadovoljstvom predstavljamo vam knjižicu sažetaka znanstveno-stručne konferencije Festung, posvećene ključnoj temi kibernetičke sigurnosti. Ova konferencija, kao i ova knjižica sažetaka, rezultat su predanog rada u sklopu projekta Cyber Festung, s ponosom financiranog od strane Europske unije i Erste banke. Njihova podrška prepoznaje vitalni značaj kibernetičke sigurnosti u suvremenom društvu te je omogućila okupljanje stručnjaka i istraživača iz različitih znanstvenih disciplina.

U digitalnom dobu, gdje su naši životi i globalni sustavi sve više isprepleteni s kibernetičkim prostorom, osiguravanje njegove sigurnosti i otpornosti imperativ je našeg vremena. Konferencija Festung stoga sjedinjuje perspektive tehničkih i društvenih znanosti, prepoznajući da je učinkovita kibernetička sigurnost složen izazov koji zahtijeva holistički pristup.

Ova knjižica sažetaka pruža uvid u bogatstvo tema i istraživanja predstavljenih na konferenciji. Obuhvaća najnovija dostignuća u tehničkim aspektima zaštite, poput naprednih kriptografskih metoda i sustava detekcije prijetnji, kao i ključne društvene dimenzije, uključujući psihologiju kibernetičke sigurnosti, utjecaj dezinformacija i socio-tehničke ranjivosti.

Vjerujemo da će ova zbirka sažetaka potaknuti plodnu razmjenu ideja, inspirirati daljnja istraživanja i doprinijeti jačanju svijesti o važnosti kibernetičke sigurnosti na svim razinama. Zahvaljujemo Europskoj uniji i Erste banci na prepoznavanju važnosti ovog područja i podršci projektu Cyber Festung, bez koje ova konferencija i ova knjižica ne bi bile moguće.

Želimo vam uspješan rad s ovom knjižicom i nadamo se da će vas inspirirati za daljnje doprinose u području kibernetičke sigurnosti.

Glavni urednik

doc. dr. sc. Mirko Cobović

Sadržaj

PROGRAM KONFERENCIJE ***19***

STRUČNJACI IZ GOSPODARSTVA ***29***

Kibernetička sigurnost u elektroenergetskim sustavima **31**
doc. dr. sc. Tomislav Alinjak, dipl. ing. el.

Sigurno korištenje interneta, zaštita podataka i digitalna pismenost među djecom i mladima **33**
Hrvoje Ćosić, bacc. oec.

Razvoj Bikademy-a uz sigurnosne izazove **35**
Krešimir Herceg, dipl. oec.

Ekonomski utjecaj digitalnih prijevara na poduzeća: Strategije za izgradnju otpornosti **37**
Tin Horvatin, mag. oec.

Pet najvećih kibernetičkih sigurnosnih rizika u sektoru zdravstvenih ustanova **39**
Zdravko Janeš, dipl.oec.

Kako kreirati učinkovitu kampanju za podizanje svijesti o kibernetičkoj sigurnosti **41**
Jakov Kiš, mag. pol. nac. sig.

Sigurnosni izazovi i mjere za njihovo prevladavanje na Sveučilištu u Slavonskom Brodu **42**
Miroslav Mazurek, mag. ing. el.

Cyber Conflict Simulator (CCS) Uvježbavanje odgovora na kibernetičke incidente i izgradnja digitalne otpornosti organizacije **44**
Goran Polonji, mag. ing.

Kibernetička sigurnost digitalnog poslovanja **45**
Gordana Prebeg, mag. oec.

Organizacija kibernetičke sigurnosti u korporativnom okruženju **47**
Marin Samardžić, mag. oec

Od ITAR regulative do domaćih izazova: Razvoj aplikacija za vojnu industriju u europskom kontekstu ____ **48**
Mladen Sudar, dipl. ing.

STRUČNJACI IZ ZNANOSTI I OBRAZOVANJA ____ ***49***

Ekonomska analiza utjecaja Direktive NIS2 na percepciju kibernetičke sigurnosti u poslovnom okruženju ____ **51**
doc. dr. sc. Mirko Cobović

Sigurnosni aspekti upravljanja znanjem ____ **53**
prof. dr. sc. Jerko Glavaš

Sigurnost i sigurnost ugrađenih računalnih sustava ____ **55**
izv. prof. dr. sc. Tomislav Matić

Kibernetička sigurnost kao poslovni resurs i alat za povećanje učinkovitosti uz primjenu umjetne inteligencije ____ **57**
doc. dr. sc. Sanela Ravlić

Optimizacija ulaganja u kibernetičku sigurnost: Ekonomska perspektiva NIS2 Direktive ____ **59**
doc. dr. sc. Lena Sigurnjak

SCADA nadzorni sustav EES s aspekta cyber sigurnosti ____ **61**
Prof. dr. sc. Marinko Stojkov

Digitalne kompetencije i sigurnost u kontekstu Industrije 4.0 ____ **63**
prof. dr. sc. Mislav Šimunić

Kibernetička sigurnost kao temelj uspješne naplate u bankarstvu ____ **65**
doc. dr. sc. Maja Vretenar Cobović

PRISTIGLE PRIJAVE ____ ***67***

Znanstveno mapiranje i trendovi istraživanja kibernetičke sigurnosti u području ekonomije i menadžmenta ____ **69**
doc. dr. sc. Višnja Bartolović, Donata Pospišil, studentica, doc. dr. sc. Milan Puvača

Gig ekonomija u Republici Hrvatskoj ____ **72**
doc. dr. sc. Ivona Blažević Dević, Marija Rossi, studentica

Prepoznavanje malicioznih napada pomoću strojnog učenja ____ **74**
Antonio Carević, student, dr. sc. Mario Dudjak, v. asist.

Sigurnosni aspekti daljinskog očitanja brojila električne energije ___ 76
Maja Čuletić Čondrić, prof. mat. i fiz., pred., Silvio Vilagoš, student, Marijana Zarožinski, dipl. ing. mat., asist.

Analiza zapošljavanja i doprinosa ICT sektora BDP-u Europske unije i Republike Hrvatske ___ 78
doc. dr. sc. Matej Galić

Kibernetička sigurnost industrijskih sustava ___ 80
Mato Galović, dipl. ing. stroj., pred., Ivan Matasović, mag. ing. el., pred., Mato Kokanović, mag. ing. el., Zoran Crnac, dipl. ing. stroj., pred.

Strojno učenje za detekciju mrežne krađe identiteta analizom URL adresa ___ 82
doc. dr. sc. Ivana Hartmann Tolić, Mirta Vujnovac, mag. educ. math. et inf.

Digitalna dekada i ekonomski rast: Kvantificiranje koristi digitalne transformacije u Europskoj uniji ___ 84
Tomislav Horvat, mag. oec., pred.

Ekonomska analiza uspješnih mobilnih marketinških kampanja sa naglaskom na sigurnost ___ 86
Josipa Jakim, studentica, doc. dr. sc. Mirko Cobović, Jasna Vujčić, prof., v. pred.

O finalnosti i istinitosti interpretacije ponašanja sustava u biologiji i informatici ___ 88
prof. dr. sc. Franjo Jović

Učestalost korištenja mobilnog bankarstva u Brodsko-posavskoj županiji ___ 90
Mirna Jurčević-Ćeranić, studentica, Jelena Meštrović, studentica, doc. dr. sc. Mirko Cobović

Etika i umjetna inteligencija: ChatGPT, kibernetička sigurnost i privatnost ___ 92
doc. dr. sc. Matilda Kolić Stanić, dr. sc. Marija Lesandrić, v. asist.

Marketinške strategije i sigurnosni izazovi u fazi lansiranja digitalnog bankarskog proizvoda ___ 94
Mirjana Kraljević, studentica, doc. dr. sc. Andreja Katolik Kovačević

Razvoj pametnih gradova ___ 96
doc. dr. sc. Anita Kulaš Mirosavljević, Valentina Vuleta, studentica

Etičnost na društvenim mrežama ___ 98
doc. dr. sc. Anita Kulaš Mirosavljević, Nikolina Matić, studentica, dr. sc. Branka Martić, pred.

Provjera znanja o kibernetičkoj sigurnosti u srednjim školama pomoću digitalnog kviza _____ 100
Ivana Lovrić Senjak, studentica, doc. dr. sc. Mirko Cobović, Žaklina Bender, prof., Anita Barišić, dipl. pead.

Ozbiljne igre o kibernetičkoj sigurnosti u kurikuluma nastave informatike _____ 102
Ivana Lovrić Senjak, studentica, Slavko Dukarić, Mihovil Gašić, student

Sigurnosni izazovi IoT uređaja _____ 104
Ivan Matasović, mag. ing. el., pred., Mato Kokanović, mag. ing. el., pred. Mato Galović, dipl. ing. stroj., pred., Zoran Crnac, dipl. ing. el., pred.

Čuvari virtualnog praga: Suočavanje s kibernetičkim prijetnjama u virtualnom turizmu _____ 106
doc. dr. sc. Igor Mavrin

Fiskalizacija 2.0: pravni okvir, digitalna transformacija i učinci na mikro i male poduzetnike u Republici Hrvatskoj _____ 108
doc. dr. sc. Ivana Miklošević

Umjetna inteligencija i kibernetička sigurnost: stavovi zaposlenika i izazovi za suvremena poduzeća _____ 110
doc. dr. sc. Ivana Miklošević, Gabrijela Bosak, studentica

Kibernetička sigurnost kao poslovna prednost: Ekonomika primjene UI sustava u nadzoru i upravljanju rizicima _____ 112
doc. dr. sc. Sanela Ravlić

Uloga kibernetičke sigurnosti u jačanju regionalne gospodarske otpornosti: institucionalne i geopolitičke perspektive _____ 114
doc. dr. sc. Sanela Ravlić, dr. sc. Ivana Unukić, v. asist.

Izgradnja otpornosti poduzeća s osvrtom na poslovne krize u digitalnom dobu _____ 116
doc. dr. sc. Lena Sigurnjak, doc. dr. sc. Sanja Knežević Kušljić, Ivana Sluganović, studentica

Modularna, performativna multimedijska umjetnost _____ 118
doc. dr. sc. Vesna Srnić

Sigurnost bolesnika tijekom liječenja u Odjelu za neurologiju _____ 120
prim. dr. sc. Lidija Šapina, dr. med. spec. neurolog, mr. sc. Krešimir Šapina, dipl. ing.

Digitalne tehnologije u obrazovanju _____ 122
izv. prof. dr. sc. Jasna Šego, dr. sc. Željka Rosandić, v. pred.

Analiza naplate plasmana poslovnih subjekata kod banaka u kontekstu kibernetičke sigurnosti _____124
doc. dr. sc. Maja Vretenar Cobović, Marina Brčelić Kovačević, studentica

Percepcije učenika o učenju temeljenom na digitalnim igrama _____126
Marijana Zarožinski, dipl. ing. mat., asist., izv. prof. dr. sc. Ljerka Jukić Matić, Maja Čuletić Čondrić, prof. mat. i fiz., pred.

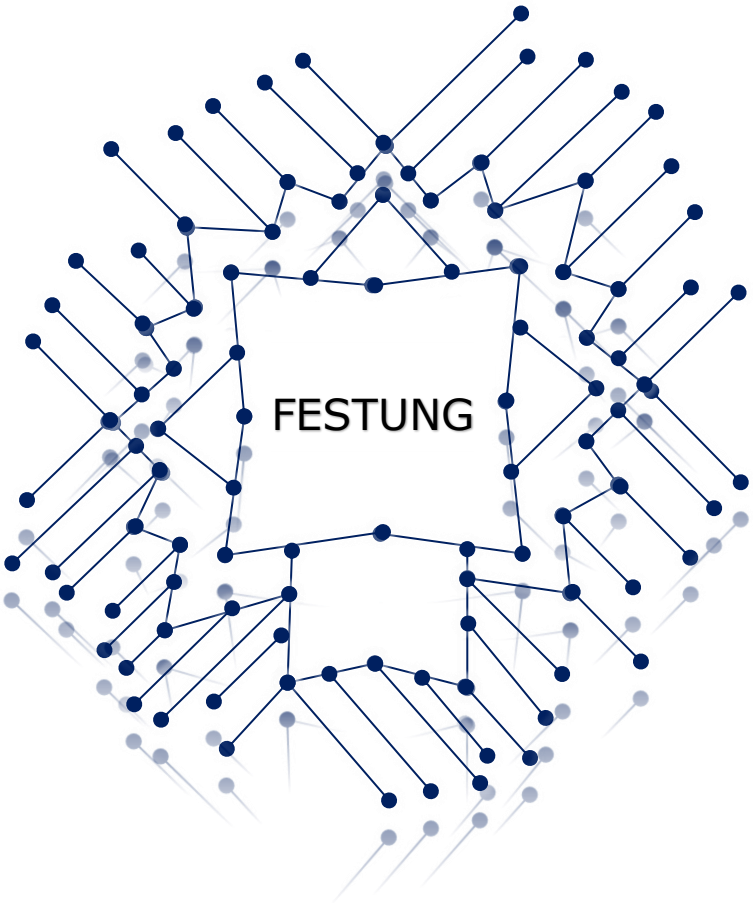
Znanstveno – stručna konferencija

FESTUNG

Slavonski Brod

11. do 13. lipnja 2025. godine

PROGRAM KONFERENCIJE



Srijeda – 11. lipnja 2025. godine

Zgrada 1, Sveučilište u Slavonskom Brodu, Trg Ivane Brlić Mažuranić 2

10:00 – 10:30 Registracija sudionika

Zgrada 1, Sveučilište u Slavonskom Brodu, Trg Ivane Brlić Mažuranić 2

Učionica 101

10:30 – 11:00 Svečano otvaranje

Pozdravni govor glavnog urednika

Pozdravni govor rektora/prorektora

Zgrada 1, Sveučilište u Slavonskom Brodu, Trg Ivane Brlić Mažuranić 2

Učionica 101

IZLAGANJA STRUČNJAKA IZ GOSPODARSTVA

11:00 – 11:15 Kibernetička sigurnost u elektroenergetskim sustavima

doc. dr. sc. Tomislav Alinjak, dipl. ing. el.

11:15 – 11:30 Sigurno korištenje interneta, zaštita podataka i digitalna pismenost među djecom i mladima

Hrvoje Ćosić, bacc. oec.

11:45 – 12:00 Razvoj Bikademy-a uz sigurnosne izazove

Krešimir Herceg, dipl. oec.

12:00 - 12:15 Ekonomski utjecaj digitalnih prijevara na poduzeća: Strategije za izgradnju otpornosti

Tin Horvatin, mag. oec.

12:15 – 12:30 Pet najvećih kibernetičkih sigurnosnih rizika u sektoru zdravstvenih ustanova

Zdravko Janeš, dipl. oec.

12:30 – 12:45 Stanka

12:45 – 13:00 Kako kreirati učinkovitu kampanju za podizanje svijesti o kibernetičkoj sigurnosti

Jakov Kiš, mag. pol. nac. sig.

13:00 – 13:15	Sigurnosni izazovi i mjere za njihovo prevladavanje na Sveučilištu u Slavonskom Brodu Miroslav Mazurek, mag. ing. el.
13:15 – 13:30	Cyber Conflict Simulator (CCS) Uvježbavanje odgovora na kibernetičke incidente i izgradnja digitalne otpornosti organizacije Goran Polonji, mag. ing.
13:30 – 13:45	Organizacija kibernetičke sigurnosti u korporativnom okruženju Marin Samardžić, mag. oec.
13:45 - 14:00	Od ITAR regulative do domaćih izazova: razvoj aplikacija za vojnu industriju u europskom kontekstu Mladen Sudar, dipl. ing.
14:00 – 15:00	Stanka za ručak

Zgrada 1, Sveučilište u Slavonskom Brodu, Trg Ivane Brlić Mažurani 2

Učionica 302

15:00 – 17:00	Radionica Cyber Conflict Simulator

Četvrtak – 12. lipnja 2025. godine

Zgrada 1, Sveučilište u Slavonskom Brodu Trg Ivane Brlić Mažuranić 2

10:00 – 10:15 Registracija sudionika

Zgrada 1, Sveučilište u Slavonskom Brodu Trg Ivane Brlić Mažuranić 2

Učionica 101

10:15 – 10:25 Pozdravni govor glavnog urednika

IZLAGANJA STRUČNJAKA IZ ZNANOSTI I OBRAZOVANJA

10:25 – 10:40 SCADA nadzorni sustav EES s aspekta cyber sigurnosti

prof. dr. sc. Marinko Stojkov pozvano predavanje

10:40 – 10:55 Sigurnost i sigurnost ugrađenih računalnih sustava

izv. prof. dr. sc. Tomislav Matić pozvano predavanje

10:55 – 11:10 Sigurnosni aspekti upravljanja znanjem

prof. dr. sc. Jerko Glavaš pozvano predavanje

11:10 – 11:25 Digitalne kompetencije i sigurnost u kontekstu Industrije 4.0

prof. dr. sc. Mislav Šimunić pozvano predavanje

11:30 – 14:00 Izlaganje po sekcijama

Zgrada 1, Sveučilište u Slavonskom Brodu Trg Ivane Brlić Mažurani ć2

Učionica 102

SEKCIJA - USMENA IZLAGANJA

11:30 – 11: 40 Kibernetička sigurnost kao temelj uspješne naplate u bankarstvu

doc. dr. sc. Maja Vretenar Cobović voditelj sekcije

11:40 – 11:50 Optimizacija ulaganja u kibernetičku sigurnost: Ekonomska perspektiva NIS2 direktive

doc. dr. sc. Lena Sigurnjak pozvano predavanje

11:50 – 12:00 Znanstveno mapiranje i trendovi istraživanja kibernetičke sigurnosti u području ekonomije i menadžmenta

doc. dr. sc. Višnja Bartolović, Donata Pospišil, studentica, doc. dr. sc. Milan Puvača

12:00 – 12:10 Prepoznavanje malicioznih napada pomoću strojnog učenja

Antonio Carević, student, dr. sc. Mario Dudjak, v. asist.

12:10 – 12:20	Kibernetička sigurnost industrijskih sustava Mato Galović, dipl. ing. stroj., pred., Ivan Matasović, mag. ing. el., pred., Mato Kokanović, mag. ing. el., Zoran Crnac, dipl. ing. stroj., pred.
12:20 – 12:30	O finalnosti i istinitosti interpretacije ponašanja sustava u biologiji i informatici prof. dr. sc. Franjo Jović
12:30 – 12:40	Učestalost korištenja mobilnog bankarstva u Brodsko-posavskoj županiji Mirna Jurčević-Ćeranić, studentica, Jelena Meštrović, studentica, doc. dr. sc. Mirko Cobović
12:40 – 12: 50	Etika i umjetna inteligencija: ChatGPT, kibernetička sigurnost i privatnost doc. dr. sc. Matilda Kolić Stanić, dr. sc. Marija Lesandrić, v. asist.
12:50 – 13:00	Marketinške strategije i sigurnosni izazovi u fazi lansiranja digitalnog bankarskog proizvoda Mirjana Kraljević, studentica, doc. dr. sc. Andreja Katolik Kovačević
13:00 – 13:10	Etičnost na društvenim mrežama doc. dr. sc. Anita Kulaš Mirosavljević, Nikolina Matić, studentica, dr. sc. Branka Martić, pred.
13:10 – 13:20	Čuvari virtualnog praga: Suočavanje s kibernetičkim prijetnjama u virtualnom turizmu doc. dr. sc. Igor Mavrin
13:20 – 13:30	Fiskalizacija 2.0: pravni okvir, digitalna transformacija i učinci na mikro i male poduzetnike u Republici Hrvatskoj doc. dr. sc. Ivana Miklošević
13:30 – 13:40	Umjetna inteligencija i kibernetička sigurnost: stavovi zaposlenika i izazovi za suvremena poduzeća doc. dr. sc. Ivana Miklošević, Gabrijela Bosak, studentica
13:40 – 13:50	Modularna, performativna multimedijska umjetnost doc. dr. sc. Vesna Srnić
13:50 – 14:00	Percepcije učenika o učenju temeljenom na digitalnim igrama Marijana Založinski, dipl. ing. mat., asist., izv. prof. dr. sc. Ljerka Jukić Matić, Maja Čuletić Čondrić, prof. mat. i fiz., pred.

Zgrada 1, Sveučilište u Slavonskom Brodu Trg Ivane Brlić Mažuranić 2

Učionica 101

SEKCIJA - ONLINE IZLAGANJA

11:30 – 11:40	Ekonomska analiza utjecaja Direktive NIS2 na percepciju kibernetičke sigurnosti u poslovnom okruženju doc. dr. sc. Mirko Cobović voditelj sekcije
11:40 – 11: 50	Kibernetička sigurnost kao poslovni resurs i alat za povećanje učinkovitosti uz primjenu umjetne inteligencije doc. dr. sc. Sanela Ravlić
11:50 – 12:00	Gig ekonomija u Republici Hrvatskoj doc. dr. sc. Ivona Blažević Dević, Marija Rossi, studentica
12:00 – 12:10	Analiza zapošljavanja i doprinosa ICT sektora BDP-u Europske unije i Republike Hrvatske doc. dr. sc. Matej Galić
12:10 – 12:20	Strojno učenje za detekciju mrežne krađe identiteta analizom URL adresa doc. dr. sc. Ivana Hartmann Tolić, Mirta Vujnovac, mag. educ. math. et inf.
12:20 – 12:30	Digitalna dekada i ekonomski rast: Kvantificiranje koristi digitalne transformacije u Europskoj uniji Tomislav Horvat, mag. oec., pred.
12:30 – 12:40	Uloga kibernetičke sigurnosti u jačanju regionalne gospodarske otpornosti: institucionalne i geopolitičke perspektive doc. dr. sc. Sanela Ravlić, dr. sc. Ivana Unukić, v. asist.
14:00 – 15:00	Stanka za ručak

Zgrada 1, Sveučilište u Slavonskom Brodu Trg Ivane Brlić Mažuranić 2

SEKCIJA - POSTER IZLAGANJA

Sigurnosni aspekti daljinskog očitanja brojila električne energije

Maja Čuletić Čondrić, prof. mat. i fiz., pred., Silvio Vilagoš, student, Marijana Zarožinski, dipl. ing. mat., asist.

Ekonomska analiza uspješnih mobilnih marketinških kampanja sa naglaskom na sigurnost

Josipa Jakim, studentica, doc. dr. sc. Mirko Cobović, Jasna Vujčić, prof., v. pred.

Razvoj pametnih gradova

doc. dr. sc. Anita Kulaš Mirosavljević, Valentina Vuleta, studentica

Provjera znanja o kibernetičkoj sigurnosti u srednjim školama pomoću digitalnog kviza

Ivana Lovrić Senjak, studentica, doc. dr. sc. Mirko Cobović, Žaklina Bender, prof., Anita Barišić, dipl. pead.

Ozbiljne igre o kibernetičkoj sigurnosti u kurikulumu nastave informatike

Ivana Lovrić Senjak, studentica, Slavko Dukarić, Mihovil Gašić, student

Sigurnosni izazovi IoT uređaja

Ivan Matasović, mag. ing. el., pred., Mato Kokanović, mag. ing. el., pred., Mato Galović, dipl. ing. stroj., pred., Zoran Crnac, dipl. ing. el., pred.

Kibernetička sigurnost kao poslovna prednost: Ekonomika primjene UI sustava u nadzoru i upravljanju rizicima

doc. dr. sc. Sanela Ravlić

Izgradnja otpornosti poduzeća s osvrtom na poslovne krize u digitalnom dobu

doc. dr. sc. Lena Sigurnjak, doc. dr. sc. Sanja Knežević Kušljić, Ivana Sluganović, studentica

Sigurnost bolesnika tijekom liječenja u Odjelu za neurologiju

prim. dr. sc. Lidija Šapina, dr. med. spec. neurolog, mr. sc. Krešimir Šapina, dipl. ing.

Digitalne tehnologije u obrazovanju

izv. prof. dr. sc. Jasna Šego, dr. sc. Željka Rosandić, v. pred.

Analiza naplate plasmana poslovnih subjekata kod banaka u kontekstu kibernetičke sigurnosti

doc. dr. sc. Maja Vretenar Cobović, Marina Brčelić Kovačević, studentica

Petak – 12. lipnja 2025. godine

Zgrada 1, Sveučilište u Slavonskom Brodu, Trg Ivane Brlić Mažuranić 2

SEKCIJA - POSTER IZLAGANJA

Sigurnosni aspekti daljinskog očitanja brojila električne energije

Maja Čuletić Čondrić, prof. mat. i fiz., pred., Silvio Vilagoš, student, Marijana Zarožinski, dipl. ing. mat., asist.

Ekonomska analiza uspješnih mobilnih marketinških kampanja sa naglaskom na sigurnost

Josipa Jakim, studentica1, doc. dr. sc. Mirko Cobović, Jasna Vujčić, prof., v. pred.

Razvoj pametnih gradova

doc. dr. sc. Anita Kulaš Mirosavljević, Valentina Vuleta, studentica

Provjera znanja o kibernetičkoj sigurnosti u srednjim školama pomoću digitalnog kviza

Ivana Lovrić Senjak, studentica, doc. dr. sc. Mirko Cobović, Žaklina Bender, prof., Anita Barišić, dipl. pead.

Ozbiljne igre o kibernetičkoj sigurnosti u kurikulumu nastave informatike

Ivana Lovrić Senjak, studentica, Slavko Dukarić, Mihovil Gašić, student

Sigurnosni izazovi IoT uređaja

Ivan Matasović, mag. ing. el., pred., Mato Kokanović, mag. ing. el., pred., Mato Galović, dipl. ing. stroj., pred., Zoran Crnac, dipl. ing. el., pred.

Kibernetička sigurnost kao poslovna prednost: Ekonomika primjene UI sustava u nadzoru i upravljanju rizicima

doc. dr. sc. Sanela Ravlić

Izgradnja otpornosti poduzeća s osvrtom na poslovne krize u digitalnom dobu

doc. dr. sc. Lena Sigurnjak, doc. dr. sc. Sanja Knežević Kušljić, Ivana Sluganović, studentica

Sigurnost bolesnika tijekom liječenja u Odjelu za neurologiju

prim. dr. sc. Lidija Šapina, dr. med. spec. neurolog, mr. sc. Krešimir Šapina, dipl. ing.

Digitalne tehnologije u obrazovanju

izv. prof. dr. sc. Jasna Šego, dr. sc. Željka Rosandić, v. pred.

Analiza naplate plasmana poslovnih subjekata kod banaka u kontekstu kibernetičke sigurnosti

doc. dr. sc. Maja Vretenar Cobović, Marina Brčelić Kovačević, studentica

Zgrada 4, Sveučilište u Slavonskom Brodu, Matije Gupca 24

10:20 – 13:30 Radionice

13:30 – 13:45 Svečano zatvaranje

Znanstveno – stručna konferencija

FESTUNG

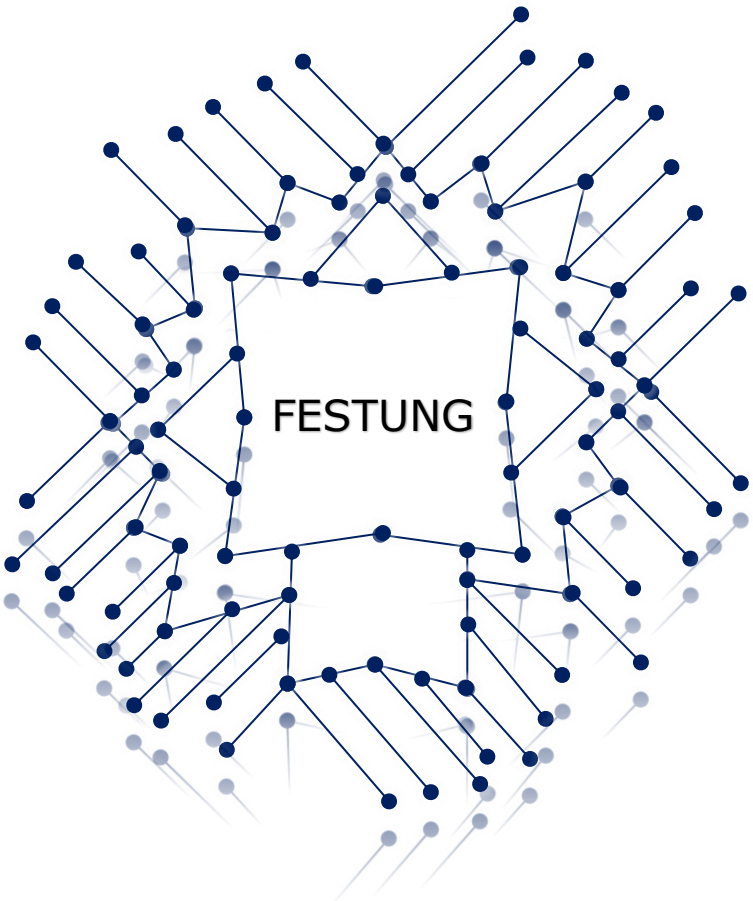
Slavonski Brod

11. do 13. lipnja 2025. godine

POZVANA PREDAVANJA

SAŽETCI

STRUČNJACI IZ GOSPODARSTVA



Kibernetička sigurnost u elektroenergetskim sustavima

Elektroenergetski sustavi se smatraju kritičnom infrastrukturom zbog velike važnosti za funkcioniranje gotovo svih djelatnosti društva. Upravljanje i nadzor sustava se sve više automatizira. Korisnici elektroenergetskog sustava sve više koriste digitalne javne usluge za razmjenu podataka i komunikaciju s operatorima sustava.

Digitalizacija i automatizacija elektroenergetskog sustava ima za posljedicu sve veću izloženost kibernetičkim ugrozama. Operator distribucijskog sustava raspolaže velikom količinom osobnih podataka o svim korisnicima koji mogu postati meta krađe podataka. Upadima u sustav može se upravljati dijelovima elektroenergetskih postrojenja što može za posljedicu imate razne sabotaže u smislu prekida napajanja.

Stoga se sve veća pažnja posvećuje zaštiti od kibernetičkih ugroza.

Predavanje će dati kratki pregled i osvrt na potencijalne opasnosti te prikazati načine na koje se ugroze sprječavaju i analiziraju.

Ključne riječi: kibernetička sigurnost, elektroenergetski sustavi

doc. dr. sc. Tomislav Alinjak, dipl. ing. el.

voditelj službe za realizaciju investicijskih projekata i pristup mreži
HEP operator distribucijskog sustava d.o.o.
ePošta: tomislav.alinjak@hep.hr

Tomislav Alinjak rođen je 18.07.1984. godine u Slavonskom Brodu.

Diplomirao je 2008. godine na Fakultetu elektrotehnike i računarstva u Zagrebu, smjer elektroenergetika – energetski sustavi, a na istom fakultetu doktorirao 2018. godine. U lipnju 2020. godine završio je sveučilišni specijalistički studij „Ekonomija energetskog sektora" na Ekonomskom fakultetu u Rijeci. Ima položen ispit IPMA razina D za voditelja projekta te je član Hrvatske komore inženjera elektrotehnike.

Od 2008. godine radi u HEP ODS d.o.o. Elektri Slavonski Brod, prvo kao koordinator poslova u odjelu za razvoj mreže, potom kao rukovoditelj odjela za razvoj i pristup mreži, zatim rukovoditelj službe za tehničke poslove te je na

trenutnoj funkciji voditelja službe za realizaciju investicijskih projekata i pristup mreži. Ponajviše se specijalizirao na poslovima vezanim uz pristup mreži, posebno distribuiranim izvorima te uz razvoj i investicije u distribucijskoj mreži.

Od 2012. do 2018. godine radio je kao vanjski suradnik u naslovnom suradničkom zvanju asistenta na Strojarskom fakultetu u Slavonskom Brodu, a kasnije napredovao do znanstveno nastavnog zvanja docenta u naslovnom zvanju.

Autor je većeg broja stručnih i znanstvenih članaka iz područja elektrotehnike te koautor jedne knjige.

Sigurno korištenje interneta, zaštita podataka i digitalna pismenost među djecom i mladima

Ovo predavanje za cilj ima podizanje svijesti o kibernetičkoj sigurnosti te osposobljavanje djece i mladih za prepoznavanje prijetnji na internetu i zaštitu svojih podataka kroz interaktivne edukativne metode.

U digitalnom okruženju prijetnje poput krađe identiteta, cyberbullyinga i dezinformacija postaju sve prisutnije, stoga je važno educirati mlade kako ih prepoznati i spriječiti. Sigurnost obuhvaća tehničke mjere zaštite, poput firewalla, antivirusnih programa i šifriranja podataka, ali i društvene aspekte sigurnosti, uključujući borbu protiv cyberbullyinga, razvoj kritičkog razmišljanja te prepoznavanje lažnih vijesti i manipulativnih sadržaja.

Poseban naglasak stavlja se na zaštitu privatnosti i osobnih podataka u skladu s GDPR regulativom te na ulogu umjetne inteligencije u prepoznavanju sigurnosnih prijetnji.

Kroz interaktivne radionice, primjere i igre, djeca se potiču na aktivno učenje i usvajanje sigurnosnih praksi. Edukacija u području kibernetičke sigurnosti ključna je za sigurno i odgovorno digitalno odrastanje, a ciljem pružanja s potrebnih znanja i alata za sigurno korištenje tehnologije.

Ključne riječi: kibernetička sigurnost, cyberbullying, zaštita podataka, medijska pismenost, digitalna privatnost.

Hrvoje Ćosić, bacc. oec.

operativni voditelj udruge Connect IT
Connect IT
ePošte: hrvoje.cosic@connect-it.hr

Hrvoje Ćosić rođen je 1983. godine u Slavonskom Brodu, gdje je završio osnovnu školu i prirodoslovno-matematički smjer Gimnazije Matija Mesić. Po zvanju je stručni prvostupnik ekonomije (smjer Menadžment), ali većinom djeluje u tehničkom području (IT I STEM) te edukativnim aktivnostima. 2008. se zapošljava kao 3D dizajner/programer u tvrtki Part Solutions LLC, gdje radi na razvoju digitalnih kataloga CAD 3D modela. 2017 prelazi u tvrtku Helioz Technologies kao CAD developer, gdje radi i danas. U udruzi Connect IT djeluje od

njenoga osnutka 2015. godine. Kao volonter edukator/mentor na području robotike, programiranja, elektronike, 3D fabrikacije i drugih STEM područja, organizirao je i održao brojne radionice za djecu i mlade, tečajeve i edukacije za učitelje i profesore osnovnih i srednjih škola, te druge edukatore iz STEM područja. Od 2023. djeluje kao operativni voditelj udruge (volonter) te koordinira svim aktivnostima udruge Connect IT.

Razvoj Bikademy-a uz sigurnosne izazove

Bikademy je jedinstvena mobilna aplikacija koja spaja cikloturizam i urbanu mobilnost kroz dva ključna segmenta: Studies i Challenges. Aplikacija motivira ljude na vožnju bicikla svakodnevno, na istraživanje destinacija biciklom i nagrađuje za to, dok prikupljeni podaci o vožnjama pružaju korisne uvide za urbanističko planiranje i održivu mobilnost.

Predavanje će predstaviti razvoj Bikademy platforme od koncepta do funkcionalnog proizvoda koji koristi više od 3.000 korisnika. Poseban naglasak bit će na kreiranju novih značajki poput Challenges, Special Studies i Special Challenges, namijenjenih kako za širu javnost, tako i za privatne tvrtke i destinacije koje žele potaknuti cikloturizam i održivu mobilnost.

Sigurnosni izazovi predstavljaju važan aspekt razvoja aplikacije, prvenstveno osiguravanje zaštite privatnih podataka korisnika, a zatim i zaštitu pristupa serveru i podacima na serveru, kao i protoka podataka između aplikacije i servera. I u tom pogledu Bikademy kontinuirano radi na poboljšanju korisničkog iskustva uz naglasak na sigurnost.

Ovo predavanje pružit će uvid u ključne trenutke razvoja Bikademy platforme, naučene lekcije te planove za daljnji rast uz konstantno unapređenje sigurnosnih aspekata.

Ključne riječi: cikloturizam, mobilnost, sigurnost, startup, IT

Krešimir Herceg, dipl. oec.

osnivač, direktor
Bikademy d.o.o.
ePošte: kherceg@gmail.com

Krešimir je osnivač Bikademy-a, proizvoda urbane mobilnosti i cikloturizma koji nagrađuje korisnike (Bikademy Studente) za svakodnevno bicikliranje te istraživanje kulturne i prirodne baštine biciklom.

Ima više od 15 godina iskustva u marketingu, aktivan je u području kulture i turizma, te je organizator brojnih događaja u tim područjima kao što je VukovART,

jedan od najvećih street art festivala u regiji. Također je kroz Udrugu Lima, čiji je predsjednik, proveo brojne EU projekte.

Zaljubljenik je u putovanja i svako slobodno vrijeme iskorištava za istraživanje novih destinacija. Uz to voli vožnje biciklom, košarku i nogomet.

Ekonomski utjecaj digitalnih prijevara na poduzeća: Strategije za izgradnju otpornosti

Mala i srednja poduzeća suočavaju se s rastućim izazovima digitalnih prijevara koje uzrokuju značajne ekonomske gubitke.

Cilj predavanja je informirati poduzetnike o ekonomskim posljedicama digitalnih prijevara i predstaviti strategije za izgradnju organizacijske otpornosti primjerene MSP sektoru.

Predavanje će analizirati tri kategorije ekonomskih gubitaka: direktne financijske gubitke, indirektne operativne troškove i dugoročne reputacijske štete. Kroz empirijske podatke i sektorske analize, identificirat će se najučestalije vrste digitalnih prijevara koje pogađaju MSP sektor, uključujući poslovne email kompromitacije, ransomware napade, prijevare s fakturama i socijalni inženjering. Na temelju studija slučaja uspješne obrane, predavanje će predstaviti višedimenzionalni okvir za izgradnju otpornosti koji obuhvaća isplative tehnološke mjere, organizacijske protokole, strategije transfera rizika i modele međuorganizacijske suradnje. Predavanje će završiti diskusijom o proaktivnom upravljanju sigurnosnim rizicima kao strateškoj komponenti dugoročne poslovne održivosti MSP-a u digitalnom okruženju.

Ključne riječi: digitalne prijevare MSP, kibernetička sigurnost, ekonomski gubitci, ransomware, organizacijska otpornost

Tin Horvatin, mag. oec.

konzultant, direktor, osnivač
Zebrica, Otprema d.o.o.
ePošta: horvatin.tin@gmail.com

Tin Horvatin, rođen 1988. u Hrvatskoj, diplomirao je na Ekonomskom fakultetu u Osijeku 2012. godine, a 2014. godine stekao naziv magistra struke (mag. oec.) na istom fakultetu. Profesionalnu karijeru započeo je kao demonstrator na Ekonomskom fakultetu u Osijeku, a paralelno je razvijao poduzetničke inicijative i stjecao iskustvo u financijama, marketingu i digitalnom poslovanju. Od 2021. radi kao predavač na Algebri d.o.o., gdje podučava kolegij "Poslovi internetskog marketinga" te od 2023. godine kao asistent na Sveučilištu u Slavonskom Brodu. Aktivan je u poduzetničkoj i stručnoj zajednici, s bogatim iskustvom u vođenju

vlastitih tvrtki, certificiranom stručnošću u digitalnom marketingu te priznanjima za inovativnost i rješavanje poslovnih izazova.

Pet najvećih kibernetičkih sigurnosnih rizika u sektoru zdravstvenih ustanova

Zdravstvene ustanove su društveno vitalno važna i složena zbirka usluga i sustava koje sudjeluju u održavanju i unapređenju javnog zdravlja i medicinske skrbi.

Od pojave interneta zdravstvene ustanove su postale glavna meta kibernetičkog kriminala te se suočavaju s brojnim sigurnosnim rizicima i prijetnjama čiji je cilj krađa i manipuliranje zdravstvenim podacima. Kako se zdravstveni sektor razvija i transformira da bi pacijentima, djelatnicima i društvu u cjelini ponudio učinkovitije i djelotvornije usluge, uz sav tehnološki napredak svakodnevno se pojavljuju i novi sigurnosni rizici i prijetnje.

Cilj predavanja je informirati i potaknuti raspravu o kibernetičkim sigurnosnim rizicima i prijetnjama s kojima se suočavaju zdravstvene ustanove.

Predavanje će analizirati pet ključnih sigurnosnih rizika koji uzrokuju sve veći broj kibernetičkih napada na računalnu infrastrukturu zdravstvenih ustanova te mjere i rješenja za uspješno savladavanje uočenih rizika i prijetnji.

Na kraju predavanja će se pokušati donijeti zaključak vezan uz skup mjera čiji je cilj postizanje kibernetički sigurne računalne infrastrukture koja omogućuje daljnji tehnološki napredak zdravstvenih ustanova kako bi svojim korisnicima mogle ponuditi brže, bolje i sigurnije zdravstvene usluge.

Ključne riječi: Kibernetička sigurnost, zdravstvene ustanove, sigurnosni rizici

Zdravko Janeš, dipl.oec.

rukovoditelj Službe za tehničke djelatnosti i informatiku
Opća bolnica "Dr. Josip Benčević"
ePošta: zdravko.janes@bolnicasb.hr

Zdravko Janeš rođen je 1973. godine u Slavonskom Brodu, diplomirao je Financijski management na Ekonomskom fakultetu u Osijeku 2006. godine. Profesionalnu karijeru započinje 1997. godine u Službi informatike u Općoj bolnici Dr .Josip Benčević u Slavonskom Brodu gdje obavlja poslove u domeni Microsoft i Linux sistemske i mrežne administracije te administracije Oracle i MS SQL Server

baza podataka. Istovremeno u sklopu radnih zadataka stječe iskustvo i u razvoju .NET Framework aplikativnih rješenja. Od 2017. godine obavlja dužnost rukovoditelja Službe tehničkih poslova i informatike u Općoj bolnici u Slavonskom Brodu. Tijekom karijere stječe brojne certifikate iz mrežne i sistemske administracije Microsoft, Cisco i Mikrotik skupine proizvoda. Kao Microsoft certificirani trener radio je kao predavač na Microsoft akademiji u sklopu Veleučilišta u Slavonskom Brodu. Trenutno kao predavač radi na Sveučilištu u Slavonskom Brodu gdje predaje na Stručnom prijediplomskom studiju Informatika i informacijske tehnologije.

Kako kreirati učinkovitu kampanju za podizanje svijesti o kibernetičkoj sigurnosti

U današnjem digitalnom svijetu, prijetnje kibernetičkoj sigurnosti rastu, a obrazovne institucije često su ciljevi napada. Ovo predavanje će vam prikazati ključne elemente kreiranja uspješne kampanje o kibernetičkoj sigurnosti unutar sveučilišnog okruženja, koristeći alate i smjernice iz ENISA-inih materijala za podizanje svijesti.

Ključne riječi: kibernetička sigurnost, awareness, podizanje svijesti

Jakov Kiš, mag. pol. nac. sig.

stručni suradnik u Odsjeku za analitiku podataka iz područja kibernetičke sigurnosti u Sektoru Nacionalnog CERT-a
CARNET: Hrvatska akademska i istraživačka mreža
ePošta: Jakov.Kis@CARNet.hr

Jakov Kiš, stručni suradnik u Odsjeku za analitiku podataka iz područja kibernetičke sigurnosti u Sektoru Nacionalnog CERT-a. Diplomirao je na Fakultetu političkih znanosti u Zagrebu. U CARNET-u radi od 2019. godine, a Sektoru Nacionalnog CERT-a pridružio se 2021. godine. Budući da je diplomirao na smjeru Nacionalne sigurnosti, odlučio se pridružiti timu Nacionalnog CERT-a kako bi se bavio kibernetičkom sigurnošću na nacionalnoj razini. U sklopu svog posla bavi se širenjem svijesti i znanja o kibernetičkoj sigurnosti, stvaranjem edukativnih materijala, vođenjem edukacija te raznim nacionalnim i međunarodnim suradnjama.

Sigurnosni izazovi i mjere za njihovo prevladavanje na Sveučilištu u Slavonskom Brodu

Predavanje će pružiti detaljan pregled mrežne infrastrukture i usluga koje Sveučilište u Slavonskom Brodu nudi svojim korisnicima. Uz analizu ključnih sigurnosnih izazova, poput zlonamjernog softvera, mrežnih ugroza i kibernetičkih napada, predavač će predstaviti konkretne mjere za njihovo prevladavanje. Fokus će biti na implementaciji vatrozida i IDS/IPS sustava, nadzoru mreže i logova, redovitim nadogradnjama sustava, izradi sigurnosnih kopija, programima edukacije o sigurnosti te fizičkoj zaštiti opreme. Cilj predavanja je pružiti praktične uvide i preporuke za poboljšanje kibernetičke sigurnosti u akademskom okruženju.

Ključne riječi: kibernetički sigurnosni izazovi i ugroze, nadzor mreže i sustava, vatrozid, zaštita od zlonamjernog softvera, obrazovanje

Miroslav Mazurek, mag. ing. el.

voditelj odsjeka za informatiku, računalnu mrežu i sigurnost
Sveučilište u Slavonskom Brodu
ePošte: mmazurek@unisb.hr

Miroslav Mazurek rođen je 11.ožujka 1963. godine u Slavonskom Brodu. Osnovnu i srednju školu završio je u Slavonskom Brodu. Diplomirao 26.travnja 1988. godine na Elektrotehničkom fakultetu u Zagrebu (danas FER), na smjeru „Radiokomunikacije i profesionalna elektronika" s radom "Izvođenje ozvučenja".

Od 15.lipnja 1988. godine zaposlen je u SOUR-u "Đuro Đaković" u Sl. Brodu, RO Tvornica vozila i opreme na poslovima i zadacima sistem analitičara (programer i projektant baza podataka).

Od 1. siječnja 1991. zaposlen na Strojarskom fakultetu Slavonski Brod sa znanstveno-nastavnim zvanjem asistent, istraživačkim zvanjem istraživač suradnik na Katedri za organizaciju i informatiku.

Od 1996. godine je u znanstveno-nastavnom zvanju stručni suradnik, istraživačkom zvanju mlađi asistent.

Od 1996. godine Hrvatska akademska istraživačka mreža – CARNet i Strojarski fakultet Slavonski Brod imenuju ga za CARNet sistem inženjera i koordinatora za Strojarski fakultet.

Od 01. ožujka 2000. godine radi na mjestu sistem inženjera. Sudjelovao je u nastavi u brojnim predmetima, koautor nekoliko znanstvenih i stručnih radova, udžbenika i skripti, sudjelovao je na znanstvenim i EU projektima te brojnim projektima suradnje s gospodarstvom. U tri mandata bio je biran u stručno tijelo Predsjedništvo vijeća korisnika CARNet-a.

Od 2018. godine je Voditelj odjela za informatiku i računalnu mrežu na Strojarskom fakultetu u Slavonskom Brodu.

Od 2020. godine Rukovoditelj Odsjeka za informatiku, računalnu mrežu i sigurnost na Sveučilištu u Slavonskom Brodu.

Cyber Conflict Simulator (CCS) Uvježbavanje odgovora na kibernetičke incidente i izgradnja digitalne otpornosti organizacije

Novo uvedeni zakonodavni okvir Zakon o kibernetičkoj sigurnosti i DORA regulativa traže od organizacija visoku razinu spremnosti za odgovor na kibernetičke incidente i krizne situacije. Ujedno smo svjedoci kako kibernetički kriminal i napredne nacionalno sponzorirane grupe provode sve više napada s značajnim posljedicama na organizacije i društvo. Kako organizacije mogu steći znanje i izgraditi vještine potrebne za takve izazove? Predavanje će dati pregled nekih od tehnika koje se mogu koristiti i ujedno prezentirati prednosti professional wargaming simulacijskog pristupa u izgradnji digitalne otpornosti organizacija. Predavanje će ujedno biti i uvod u radionicu „Odgovor na kibernetičke incidente" koja će se održati tijekom konferencije.

Ključne riječi: Kibernetička sigurnost, Kibernetički incidenti, Uvježbavanje odgovora na incidente, Krizno upravljanje, Wargaming

Goran Polonji, mag. ing.

Cybersecurity & IT auditor, Security consultant and Co-Founder at Utilis Ltd.
Utilis d.o.o.
ePošte: goran.polonji@utilis.biz

Gordana Prebeg, rođena je 1978. u Slavonskom Brodu, diplomirala je kao magistar Goran Polonji mag.ing. CISA je konzultant za informacijsku sigurnost i revizor kibernetičke sigurnosti s preko 20 godina iskustva u radu s financijskim institucijama i različitim sektorima industrije na poboljšanju informacijske sigurnosti i osiguranju usklađenosti sa zakonodavnim okvirom. Kao stručnjak za domenu kibernetičke sigurnosti, Goran je ključni član razvojnog tima Cyber Conflict Simulatora platforme za uvježbavanje odgovora na kibernetičke incidente i krize. Tijekom svoje karijere fokusiran je izgradnju razumijevanja između upravljačkih funkcija i tehnoloških stručnjaka u području izazova kibernetičke sigurnosti. Kao konzultant Goran je posvećen harmonizaciji administrativnih i tehničkih sigurnosnih kontrola, pomažući organizacijama da ojačaju digitalnu otpornost u okruženju rastućih kibernetičkih prijetnji.

Kibernetička sigurnost digitalnog poslovanja

Računovodstveno i administrativno poslovanje gotovo je u potpunosti digitalizirano. Novi propisi iz područja digitalizacije poslovanja „Fiskalizacija 2.0" dodatno obvezuju sve poduzetnike na razmjenu svih financijskih dokumenata isključivo putem interneta. Iako su sustavi za B2B, B2C i B2G razmjenu podataka uglavnom sigurni, prelazak na isključivo online poslovanje predstavljat će značajan rizik za kibernetičku sigurnost poduzeća. Čak i poduzeća koja su do sada imala zatvorene IT sustave (kojima se ne može pristupati putem interneta) u skoroj budućnosti morati će svoje osjetljive podatke dostavljati putem interneta.

Najslabija sigurnosna karika u svakom sustavu su korisnici IT sustava (poduzetnici, računovođe i zaposlenici), a izazovi osiguranja od kibernetičkih napada su sve veći.

Cilj predavanja je ukazati na povećane rizike za kibernetičku sigurnost, osvijestiti važnost edukacije u navedenom području te na primjerima pokazati neke od trenutno dostupnih usluga zaštite i kibernetičke sigurnosti, te na koji na koji način računovodstveni servisi mogu smanjiti sigurnosne rizike. Predavanje će analizirati mogućnosti za identifikaciju i prevenciju sigurnosnih propusta, otkrivanje anomalija ili zlonamjernog ponašanja korisnika, sigurnosne kontrole i načine njihove implementaciju u poslovne procese povezane uz računovodstvo i administrativno poslovanje.

Predavanje će završiti diskusijom i sumiranjem ključnih zaključaka, s ciljem podizanja svijesti o važnosti ulaganja u zaštitu poslovanja i sprječavanje šteta nastalih zbog sigurnosnih kibernetičkih propusta.

Ključne riječi: Kibernetička sigurnost, računovodstvo, zaštita od kibernetičkih napada

Gordana Prebeg, mag. oec.

projekt menadžer, konzultant
CountIT d.o.o.
ePošte: gordana@countit.hr

Gordana Prebeg, rođena je 1978. u Slavonskom Brodu, diplomirala je kao magistar ekonomije na Veleučilištu u Slavonskom Brodu 2018. godine. Od 2019. godine je asistentica na Sveučilištu u Slavonskom Brodu za znanstveno područje Društvenih

znanosti, polje Ekonomija. Profesionalnu karijeru ostvaruje u sektoru računovodstva od 1996. godine do danas. Uz računovodstvo godinama radi u informatičkom sektoru, od 2009. godine u tvrtci Infolink d.o.o., a zatim od 2013. godine u vlastitoj tvrtci Count IT d.o.o. za računovodstvo i informatiku. Aktivna je u znanstvenim i stručnim krugovima, u razvoju projekata u lokalnoj zajednici, te je jedan od idejnih začetnika i osnivača udruge Connect IT za razvoj IKT sektora. Često kao predavač sudjeluje na izlaganjima, predavanjima i konferencijama.

Organizacija kibernetičke sigurnosti u korporativnom okruženju

U modernom informacijskom dobu, poslovni subjekti suočavaju se s rastućim kibernetičkim prijetnjama usmjerenim na infrastrukturu i identitete. Ovo predavanje pružit će uvid u strukturu i organizaciju obrane od takvih prijetnji unutar poslovnog okruženja. Fokus će biti na strukturi ljudskih resursa i organizaciji timova za kibernetičku sigurnost, ključnim procesima te tehničkim rješenjima. Teme će obuhvatiti sigurnost identiteta, uređaja, mreža i aplikacija, kao i procedure za alarmiranje i rješavanje sigurnosnih incidenata. Poseban naglasak bit će stavljen na razliku između organizacijske i tehničke sigurnosti.

Ključne riječi: Kibernetička sigurnost, struktura i organizacija, identiteti

Marin Samardžić, mag. oec.

Security Team
Tipico Sports Services d.o.o.
ePošta: marin.samardzic@tipico.com

Marin Samardžić (rođen 1980. godine) diplomirao je ekonomiju (stručni specijalist ekonomije) na Sveučilištu u Slavonskom Brodu 2021. godine, a prethodno je stekao zvanje inženjera prometa na Tehničkom Veleučilištu u Zagrebu. Profesionalnu karijeru u IT sektoru započeo je 2001. godine. Od 2005. do 2011. radio je u tvrtki ProSoft na održavanju IT infrastrukture i mreža. Od 2011. do sredine 2022. godine radio je u tvrtki Sport-Bet (danas Tipico), gdje je napredovao od inženjera za IT infrastrukturu do voditelja tima za IT infrastrukturu i podršku. Sredinom 2022. godine prelazi u odjel za korporativnu sigurnost, gdje je član tima za informacijsku sigurnost, fokusirajući se na identitete, uređaje, mreže i incidente. Njegovo dugogodišnje iskustvo u IT infrastrukturi i prelazak u tim za informacijsku sigurnost čini ga relevantnim za rasprave o praktičnoj primjeni sigurnosnih mjera u IT okruženjima, upravljanju incidentima i zaštiti IT sustava.

Od ITAR regulative do domaćih izazova: razvoj aplikacija za vojnu industriju u europskom kontekstu

Predavanje je temeljeno na praktičnom iskustvu razvoja aplikacija unutar okvira ITAR regulative (International Traffic in Arms Regulations – američki propisi o kontroli izvoza vojne i obrambene tehnologije), s ciljem razmjene znanja o sigurnosnim zahtjevima, organizacijskim ograničenjima i infrastrukturnim izazovima u razvoju softvera za osjetljive sektore. Bit će predstavljeni konkretni problemi poput kontrole pristupa, zaštite intelektualnog vlasništva, sigurnosti podataka i distribucije softvera u decentraliziranim okruženjima, s osvrtom na razliku između američkih i europskih sigurnosnih standarda. U fokusu su izazovi u Hrvatskoj i EU, gdje takva razina sigurnosne discipline često izostaje. Kroz osobni primjer rada na ITAR-reguliranim sustavima te razvoj patenta za detekciju dijelova elektroničkih komponenti, predavanje otvara pitanje: kako se u Hrvatskoj pristupa razvoju osjetljivih tehnologija, tko preuzima odgovornost za sigurnost i gdje započinje promjena?

Ključne riječi: ITAR, sigurnost aplikacija, decentralizirani sustavi

Mladen Sudar, dipl. ing.

Chief Visionary & Success Officer
Helioz Technologies
ePošta: mladen@heliozgroup.com

Mladen Sudar je poduzetnik i tehnološki lider s više od 20 godina iskustva u razvoju složenih softverskih sustava. Direktor je četiri tehnološke tvrtke, uključujući Simpert j.d.o.o. Vodi strateške inicijative u Helioz Technologies, fokusirane na digitalnu transformaciju i napredne CPQ sustave. Predsjednik je udruge Connect IT, koja promovira razvoj informatičke pismenosti i digitalnih vještina u obrazovanju. Njegov rad obuhvaća upravljanje razvojnim operacijama, vizualnu komunikaciju i usklađenost s regulativama poput ITAR-a (International Traffic in Arms Regulations) u europskom kontekstu. Fokusiran je na sigurnost podataka, inovacije u ICT sektoru i uspostavu robusnih sustava za industrijsku primjenu.

Znanstveno – stručna konferencija

FESTUNG

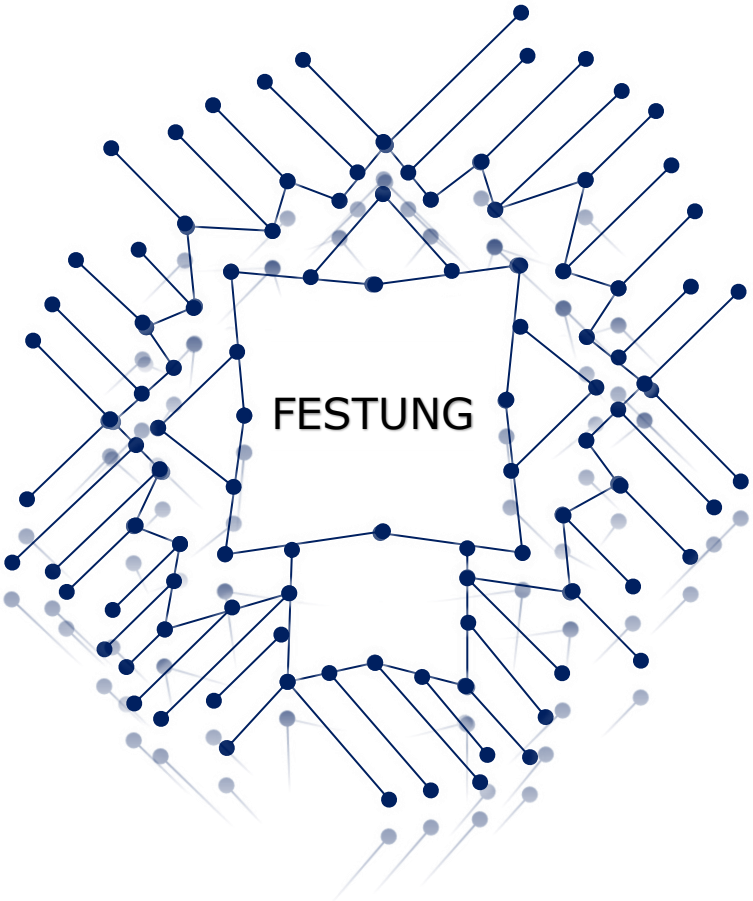
Slavonski Brod

11. do 13. lipnja 2025. godine

POZVANA PREDAVANJA

SAŽETCI

STRUČNJACI IZ ZNANOSTI I OBRAZOVANJA



Ekonomska analiza utjecaja Direktive NIS2 na percepciju kibernetičke sigurnosti u poslovnom okruženju

Ovo predavanje bavi se ključnim ekonomskim aspektima implementacije Direktive NIS2 unutar poslovnog okruženja. Analizirati će se financijski troškovi koje ova direktiva nameće različitim tipovima poslovnih subjekata. Nadalje, procijenit će se kako će NIS2 utjecati na razinu investicija u kibernetičku sigurnost te razmotriti potencijalne ekonomske prednosti koje proizlaze iz smanjenja izloženosti kibernetičkim rizicima.

Tijekom predavanja pokazati će se financijski poticaji i prepreke s kojima se tvrtke susreću prilikom usklađivanja s novim zahtjevima. Također raspraviti će se o dugoročnim posljedicama Direktive NIS2 na tržište kibernetičkih proizvoda i usluga.

Ovo predavanje ima za cilj pružiti poslovnim liderima i kreatorima politike jasnu ekonomsku argumentaciju za ulaganje u kibernetičku sigurnost u kontekstu Direktive NIS2.

Ključne riječi: Ekonomska analiza, Direktiva NIS2, Kibernetička sigurnost

doc. dr. sc. Mirko Cobović

Sveučilište u Slavonskom Brodu
Odjel društveno-humanističkih znanosti, Odsjek za ekonomiju
ePošta: mcobovic@unisb.hr

Životni put Mirka Cobovića, rođenog 1984. godine u Slavonskom Brodu, karakterizira interdisciplinarni pristup znanju i profesionalnom razvoju. Njegova akademska formacija započinje diplomom inženjera elektrotehnike koju stječe 2008. godine na Elektrotehničkom fakultetu u Osijeku, čime postavlja temelje za razumijevanje tehničkih sustava i inovacija. No, njegova znatiželja nije se zaustavila na inženjerskim znanostima. Prepoznajući važnost upravljačkih vještina u suvremenom poslovnom okruženju, 2010. godine završava specijalistički studij organizacije i managementa na Ekonomskom fakultetu u Osijeku, stječući titulu sveučilišnog specijaliste. Vrhunac njegove formalne edukacije predstavlja doktorat iz područja ekonomije, s fokusom na računalstvo u oblaku, koji je obranio 2021. godine na istom fakultetu. Ova disertacija svjedoči o njegovoj sposobnosti

integriranja tehničkog znanja s ekonomskim i upravljačkim perspektivama, čime se pozicionira kao stručnjak na raskrižju različitih disciplina.

Profesionalnu karijeru započinje kao nastavnik računalstva u Tehničkoj školi u Slavonskom Brodu, prenoseći svoje znanje mladim naraštajima. Paralelno s tim, stječe praktično iskustvo radeći u tvrtki ProSoft d.o.o., čime obogaćuje svoj profesionalni profil. Od 2009. godine svoje profesionalno djelovanje nastavlja na Veleučilištu u Slavonskom Brodu, gdje napreduje od informatičara-stručnog suradnika do višeg predavača, aktivno sudjelujući u akademskom životu i obrazovanju studenata. Njegova predanost i kompetentnost prepoznate su i na Sveučilištu u Slavonskom Brodu, gdje je 2023. godine izabran u znanstveno nastavno zvanje docenta, čime potvrđuje svoju relevantnost u visokoškolskom sustavu.

Mirko Cobović je aktivan sudionik znanstvenih i stručnih krugova. Svoje spoznaje i rezultate istraživanja redovito prezentira na brojnim izlaganjima, a njegov doprinos znanstvenoj zajednici očituje se i kroz publikacije te sudjelovanje u različitim projektima. Njegova interdisciplinarna pozadina i kontinuirano usavršavanje čine ga vrijednim članom akademske zajednice i relevantnim stručnjakom u područjima kojima se bavi.

Sigurnosni aspekti upravljanja znanjem

Upravljanje znanjem postaje ključni čimbenik uspjeha suvremenih organizacija koje se suočavaju s brzim tehnološkim promjenama i rastućom količinom podataka. Međutim, dok učinkovito upravljanje znanjem može povećati inovativnost i konkurentnost, istovremeno otvara niz sigurnosnih izazova. Ovaj rad istražuje sigurnosne aspekte upravljanja znanjem, s posebnim naglaskom na zaštitu povjerljivih informacija, intelektualnog vlasništva te sigurnost digitalnih sustava za pohranu i dijeljenje znanja. Analiziraju se prijetnje poput neovlaštenog pristupa, curenja podataka te rizika povezanih s ljudskim faktorom. Također se razmatra uloga sigurnosnih politika, enkripcije, kontrole pristupa i edukacije zaposlenika u prevenciji sigurnosnih incidenata. Kroz pregled literature i primjere iz prakse, rad ističe važnost integracije sigurnosnih mjera u sve faze ciklusa upravljanja znanjem – od prikupljanja i pohrane do distribucije i primjene. Zaključno, sigurnost upravljanja znanjem ne smije se promatrati kao tehničko pitanje već kao sastavni dio organizacijske strategije koja osigurava dugoročnu održivost i zaštitu konkurentskih prednosti.

Ključne riječi: Upravljanje, znanje, upravljanje znanjem, sigurnost

prof. dr. sc. Jerko Glavaš

Sveučilište J.J. Storssmayera u Osijeku
Ekonomski fakultet u Osijeku
ePošta: jerko.glavas@efos.hr

Prof. dr. sc. Jerko Glavaš (rođen 1981. u Osijeku) je doktor ekonomskih znanosti s Ekonomskog fakulteta u Osijeku, gdje radi od 2006. godine. Aktivno je uključen u akademsku zajednicu kroz stalnu suradnju i recenziranje za brojne konferencije u zemlji i inozemstvu, gdje redovito dijeli svoja znanja i uvide. S bogatim iskustvom sudjelovanja na više od 100 domaćih i međunarodnih konferencija, prof.dr.sc. Glavaš je prepoznat kao relevantan stručnjak u svom području. Također je član uredništva nekoliko časopisa i zbornika radova, čime doprinosi diseminaciji znanstvenih spoznaja. Uz akademski rad, prof.dr.sc. Glavaš posjeduje relevantno iskustvo u području sigurnosti kroz svoje članstvo u odborima i društvima, gdje je često obnašao i dužnosti predsjednika. Njegovo razumijevanje kompleksnih sustava i upravljanja rizicima, stečeno kroz akademsku karijeru i praktični angažman, čini ga vrijednim predavačem na konferencijama koje se dotiču

ekonomskih i sigurnosnih aspekata poslovanja. Aktivan je i u brojnim strukovnim udrugama te je predavač na više visokoškolskih institucija..

Sigurnost i sigurnost ugrađenih računalnih sustava

Cilj predavanja je istaknuti važnost sigurnosti (engl. safety) i sigurnosti (engl. security) u ugrađenim računalnim sustavima, s naglaskom na standarde, primjenu i izazove sigurnosno kritičnih sustava.

Računalni sustavi su sveprisutni oko nas, u našim domovima, automobilima, na radnom mjestu, kada šetamo, kada se zabavljamo... Ovo predavanje obrađuje dualnu prirodu sigurnosti ugrađenih računalnih sustava – fizičku sigurnost (engl. safety) koja sprječava nesreće i štetu koja može nastati upotrebom istih, te sigurnost informacija (engl. security) koja štiti takve sustave od zlonamjernih napada. Definiraju se svojstva koja trebaju ispunjavati sigurnosni sustavi. Posebna pozornost posvećena je SIL standardima (engl. Safety Integrity Level) za pojedine kategorije proizvoda te se razmatraju primjene u automobilskoj industriji, automatizaciji i kritičnoj infrastrukturi s naglaskom na ugrađene računalne sustave. Predavanje također adresira suvremene prijetnje povezane s IoT uređajima, bežičnim komunikacijama i primjenom takvih sustava u komercijalne svrhe te predstavlja metode povećanja sigurnosti ugrađenih računalnih sustava.

Ključne riječi: fizička sigurnost, sigurnost informacija, IoT uređaji, SIL standardi, povećanje sigurnosti.

izv. prof. dr. sc. Tomislav Matić

Sveučilište J.J. Storssmayera u Osijeku
Fakultet elektrotehnike, računarstva i informacijskih tehnologija
ePošta: tomislav.matic1@ferit.hr

Izv. prof. dr. sc. Tomislav Matić (rođen 1983. u Brčkom, BiH) diplomirao je elektrotehniku (2007.) na Elektrotehničkom fakultetu Osijek, gdje je 2014. godine doktorirao iz područja računarstvo. Danas radi kao izvanredni profesor na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija Osijek, gdje predaje kolegije vezane za razvoj sklopovlja. Kao aktivan istraživač, sudjeluje na brojnim međunarodnim i domaćim projektima te objavljuje radove iz područja ugrađenih računalnih sustava, sustava stvarnog vremena i obrade slike. Uveo je nekoliko novih kolegija i koautor je sveučilišnih udžbenika. Izv. prof. dr. sc. Matić također je aktivan u promociji znanosti. S obzirom na njegovo područje ekspertize

u razvoju sklopovlja i ugrađenim sustavima, Izv. prof. dr. sc. Matić posjeduje značajna znanja vezana uz sigurnosne aspekte računalnih sustava na niskoj razini i pouzdanost hardvera. Njegovo iskustvo u dizajnu i analizi pouzdanosti sklopovlja čini ga relevantnim predavačem na konferencijama koje se dotiču sigurnosti ugrađenih sustava i hardverskih ranjivosti.

Kibernetička sigurnost kao poslovni resurs i alat za povećanje učinkovitosti uz primjenu umjetne inteligencije

Ovo predavanje analizira ekonomske implikacije primjene naprednih sustava kognitivnog video nadzora. Sustav temeljen na umjetnoj inteligenciji i strojnom učenju značajno mijenja paradigmu sigurnosti – od tradicionalne tjelesne i tehničke zaštite prema automatiziranom, prediktivnom i inteligentnom nadzoru.

Kroz ekonomski pristup raspravit će se omjer ulaganja i koristi (ROI) implementacije takvih sustava, uključujući direktne uštede u operativnim troškovima (npr. smanjenje potrebe za fizičkim nadzorom) i neizravne koristi poput smanjenja šteta, gubitaka i pravne izloženosti. Poseban fokus stavlja se na mogućnosti koje ovakvi sustavi donose menadžmentu kroz integraciju s informacijskim sustavima (MIS), kao i njihovu ulogu u upravljanju rizicima i osiguravanju usklađenosti s regulatornim okvirom (npr. GDPR, NIS2). Bit će predstavljeni primjeri iz više sektora, s naglaskom na skalabilnost rješenja, fleksibilnost primjene i koristi za operativni menadžment.

Predavanje ima za cilj pružiti poslovnim liderima, stručnjacima za sigurnost i donositeljima odluka jasnu ekonomsku argumentaciju za strateško ulaganje u sustave umjetne inteligencije u funkciji sigurnosti, analitike i operativne optimizacije.

Ključne riječi: kibernetička sigurnost, ekonomika sigurnosti, umjetna inteligencija

doc. dr. sc. Sanela Ravlić

Sveučilište u Slavonskom Brodu
Odjel društveno-humanističkih znanosti, Odsjek za ekonomiju
ePošta: sravlic@unisb.hr

Doc. dr. sc. Sanela Ravlić je docentica na Sveučilištu u Slavonskom Brodu i vanjska suradnica na Veleučilištu Baltazar Zaprešić. Doktorirala je na Ekonomskom fakultetu u Osijeku, gdje je i ranije diplomirala marketing menadžment. Njeno znanstveno i stručno djelovanje obuhvaća područja ekonomije, menadžmenta,

upravljanja znanjem i informacijskim sustavima, s posebnim fokusom na utjecaj digitalnih alata na organizacijsku učinkovitost, zapošljivost i regionalni razvoj.

Autorica je i suautorica više znanstvenih radova i knjiga, uključujući teme poslovne inteligencije, mobilnosti radne snage i upravljanja resursima u ruralnim područjima. Sudjelovala je na brojnim međunarodnim znanstvenim konferencijama te kao istraživačica na projektima usmjerenima na javnu upravu, interne komunikacije i digitalnu transformaciju. Vodila je niz EU projekata vezanih uz zapošljavanje, obrazovanje i društveni razvoj.

U svom radu spaja interdisciplinarni pristup, uključujući menadžment, informacijske sustave i javne politike, s ciljem stvaranja održivih i inovativnih modela razvoja lokalnih zajednica i obrazovnih institucija.

Optimizacija ulaganja u kibernetičku sigurnost: Ekonomska perspektiva NIS2 Direktive

Ovo predavanje bavi se ključnim ekonomskim aspektima implementacije Direktive NIS2 unutar poslovnog okruženja. Analizirati će se financijski troškovi koje ova direktiva nameće različitim tipovima poslovnih subjekata. Nadalje, procijenit će se kako će NIS2 utjecati na razinu investicija u kibernetičku sigurnost te razmotriti potencijalne ekonomske prednosti koje proizlaze iz smanjenja izloženosti kibernetičkim rizicima.

Tijekom predavanja pokazati će se financijski poticaji i prepreke s kojima se tvrtke susreću prilikom usklađivanja s novim zahtjevima. Također raspraviti će se o dugoročnim posljedicama Direktive NIS2 na tržište kibernetičkih proizvoda i usluga.

Ovo predavanje ima za cilj pružiti poslovnim liderima i kreatorima politike jasnu ekonomsku argumentaciju za ulaganje u kibernetičku sigurnost u kontekstu Direktive NIS2.

Ključne riječi: NIS2 direktiva, ekonomska analiza, kibernetička sigurnost

doc. dr. sc. Lena Sigurnjak

Sveučilište u Slavonskom Brodu
Odjel društveno-humanističkih znanosti, Odsjek za ekonomiju
ePošta: lsigurnjak@unisb.hr

Rođena u Slavonskom Brodu 1984. godine, Lena Sigurnjak od ranih je dana pokazivala sklonost prema znanju i usavršavanju. Nakon završene opće gimnazije Matija Mesić u rodnom gradu 2003. godine, njezina akademska znatiželja vodila ju je prema Zagrebu, gdje upisuje Zagrebačku školu ekonomije i managementa. Diplomiravši 2007. godine, Lena je s entuzijazmom nastavila svoje obrazovanje, upisavši 2008. godine Specijalistički poslijediplomski studij Strateško poduzetništvo na Ekonomskom fakultetu u Zagrebu, gdje 2011. stječe zvanje sveučilišne specijalistice ekonomije.

Njezina žeđ za znanjem nije jenjavala, te iste godine upisuje poslijediplomski doktorski studij Management na Ekonomskom fakultetu u Osijeku, kulminirajući doktoratom 2016. godine. Posvećenost pedagoškim kompetencijama ogleda se u

završetku Programa pedagoško-psihološke i didaktičko-metodičke izobrazbe na Fakultetu za odgojne i obrazovne znanosti u Osijeku 2017. godine, čime je dodatno osnažila svoje nastavničke vještine.

Osim formalnog obrazovanja, Lena je aktivno ulagala u svoje usavršavanje pohađajući prestižne svjetske poslovne škole. Njezina akademska putovanja uključuju boravke na Università Bocconi u Milanu 2004., International University in Moscow 2006., Rennert Bilingual School u New Yorku 2007. te Ted Bauer School of Business na Houston Universityju 2009. godine. Ova međunarodna iskustva obogatila su njezinu perspektivu i proširila njezinu mrežu kontakata.

Profesionalnu karijeru započinje 2010. godine na Veleučilištu u Slavonskom Brodu, gdje je svojim predanim radom stekla zvanje profesora stručnog studija. Od 2020. godine nastavlja svoj profesionalni put kao docentica na Odjelu društveno humanističkih znanosti / Odsjeku za ekonomiju Sveučilišta u Slavonskom Brodu. Njezina posvećenost znanstvenom radu očituje se u značajnom broju objavljenih znanstvenih i stručnih radova iz područja ekonomije te aktivnom sudjelovanju na brojnim međunarodnim znanstvenim skupovima. Glavna područja njezina istraživačkog interesa obuhvaćaju mikroekonomiju, poduzetništvo i strateški menadžment.

Kroz svoju akademsku i profesionalnu karijeru, Lena Sigurnjak pokazuje iznimnu predanost obrazovanju, znanstvenom istraživanju i kontinuiranom usavršavanju, čime značajno doprinosi akademskoj zajednici i razvoju znanja u području ekonomije.

SCADA nadzorni sustav EES s aspekta cyber sigurnosti

U elektroenergetskom sustavu primjena SCADA sustava je široka od elektrana, sustava elektrana, sustava prijenosa i sustava distribucije električne energije. SCADA sustavi u EES (svaki EES je široko rasprostranjen s velikim udaljenostima između centralne stanice i pojedinih RTU) omogućuju generiranje velikog broja i vrste izvještaja vezanih uz proizvodnju, prijenos i/ili distribuciju električne energije sa različitih razina upravljanja (vođenje pogona, planiranje investicija, održavanje, parametriranje zaštite, analiza poslovanja) koji su temelj za strateško upravljanje EES pa su posljedično ovi SCADA sustavi i najsloženiji i najveće vrijednosti.

Kako u današnjem svijetu postoji velika prijetnja od cyber terorizma, iznimno je važno pitanje vezano uz ranjivost računalnih nadzornih SCADA sustava u funkciji upravljanja sustavima za distribuciju vode, naftovoda, plinovoda i EES. Svaki SCADA sustav je manje ili više podložan cyber napadu ovisno o integriranim karakteristikama predmetnog SCADA sustava. Arhitektura SCADA sustava je evoluirala tijekom vremena usporedo s razvojem računalnih mreža i unapređivanjem sigurnosnih komunikacijskih protokola. Iako su suvremeni projekti SCADA sustava fleksibilniji i funkcionalniji, i dalje su ranjivi na ove prijetnje. Takav napad na SCADA sustav može doći iz samog sustava (preko direktnog pristupa na sklopovlje SCADA sustava) ali može doći i iz vanjskog izvora preko komunikacijske infrastrukture. Uvijek je osnovni cilj smanjivanje mogućnosti ili potpuno eliminiranje zlonamjernih cyber napada. Napadači žele probiti zaštitu odnosno engl. firewall sustava.

Ključne riječi: SCADA, daljinsko mjerenje, nadzor, elektroenergetski sustav, cyber sigurnost

Prof. dr. sc. Marinko Stojkov

Sveučilište u Slavonskom Brodu
Strojarski fakultet u Slavonskom Brodu
ePošta: mstojkov@unisb.hr

Prof. dr. sc. Marinko Stojkov (rođen 1970. u Slavonskom Brodu) diplomirao je (1994.), magistrirao (1998.) i doktorirao (2002.) elektrotehniku na Fakultetu elektrotehnike i računarstva u Zagrebu. Profesionalnu karijeru započeo je u HEP Elektra Slavonski Brod te je radio kao nastavnik na Elektrotehničkom fakultetu u Osijeku. Od 2009. radi na Strojarskom fakultetu u Slavonskom Brodu, gdje je

napredovao do redovitog profesora u trajnom zvanju. S bogatim iskustvom vođenja preko stotinu projekata u suradnji s gospodarstvom, prof. dr. sc. Stojkov posjeduje značajna znanja relevantna za područje sigurnosti elektroenergetskih sustava, stečena kroz rad u HEP Elektri i na brojnim projektima. Njegova ekspertiza u implementaciji i upravljanju složenim tehničkim sustavima čini ga relevantnim predavačem na konferencijama koje se dotiču tehničkih aspekata i sigurnosnih izazova u elektroenergetici. Objavio je preko stotinu znanstvenih radova.

Digitalne kompetencije i sigurnost u kontekstu Industrije 4.0

Digitalna transformacija industrije, poznata kao Industrija 4.0, intenzivno mijenja tržište rada nameću nove zahtjeve prema digitalnim kompetencijama stručnjaka, posebice u području cyber sigurnosti. U tom kontekstu nameće se potreba provođenja istraživanja usklađenosti/diskrepancije između digitalnih kompetencija, koje studenti stječu kroz visokoobrazovne programe te kompetencija koje tržište rada stvarno zahtijeva u kontekstu Industrije 4.0. Osim studenata, naglašava se važnost kontinuiranog usavršavanja nastavnika u visokom obrazovanju, koji moraju sustavno razvijati svoje digitalne kompetencije kako bi bili sposobni učinkovito prenositi nova znanja studentima, prateći brze tehnološke promjene. Istraživanja bi se trebala oslanjati na europski okvir digitalnih kompetencija (DigComp), u kojem sigurnost predstavlja jednu od ključnih komponenti. Dosadašnja istraživanja pokazuju potrebu sustavne integracije kompetencija cyber sigurnosti u obrazovne programe i trajnog obrazovanja nastavnika. Prateći taj trend doprinijet će se smanjenju jaza između obrazovnih ishoda i potreba tržišta rada, a povećat će se konkurentnost diplomiranih studenata i osigurati sigurna i održiva digitalna transformacija okviru gospodarstva.

Ključne riječi: visoko obrazovanje, digitalne kompetencije, sigurnost, Industrija 4.0

prof. dr. sc. Mislav Šimunić

Sveučilište u Rijeci
Fakultet za menadžment u turizmu i ugostiteljstvu
ePošta: **mislavs@fthm.hr**

Prof.dr.sc. Mislav Šimunić (rođen 1971. u Rijeci) doktorirao je (2004.) na Fakultetu organizacije i informatike u Varaždinu. S gotovo 30 godina iskustva u sustavu znanosti i visokog obrazovanja, danas radi kao redoviti profesor u trajnom zvanju na Fakultetu za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci. Njegova stručnost obuhvaća primjenu informacijsko-komunikacijskih tehnologija u turizmu i visokom obrazovanju, s fokusom na digitalnu transformaciju i e-poslovanje. Kao nositelj više kolegija na preddiplomskom, diplomskom i doktorskom studiju, prof.dr.sc. Šimunić aktivno doprinosi obrazovanju stručnjaka.

Njegov znanstveno-istraživački rad usmjeren je na digitalnu transformaciju, e-poslovanje i internetski marketing, a autor je i koautor brojnih publikacija. Kroz sudjelovanje u nacionalnim i međunarodnim projektima te recenzentski rad u uglednim časopisima, aktivan je u znanstvenoj zajednici. S obzirom na njegovu ekspertizu u digitalnim tehnologijama i e-poslovanju, prof. dr. sc. Šimunić posjeduje relevantno znanje o sigurnosnim aspektima digitalnog poslovanja i zaštiti podataka u turizmu. Njegovo iskustvo u primjeni suvremenih tehnoloških rješenja čini ga relevantnim predavačem na konferencijama koje se bave digitalizacijom i sigurnosnim izazovima u turističkom sektoru.

Kibernetička sigurnost kao temelj uspješne naplate u bankarstvu

U današnjem dinamičnom svijetu bankarstva, uspješna naplata plasmana prema poslovnim subjektima suočava se s novim izazovima – onima proizašlim iz kibernetičkih prijetnji. Svaka komunikacija, svaki korak u procesu naplate dugoročnih i kratkoročnih kredita, revolving kredita ili garancija, sve je više pod lupom potencijalnih kibernetičkih napada.

Ovo predavanje će istražiti kako ključni proces naplate u bankarstvu postaje ranjiv na digitalne prijetnje te zašto je kibernetička sigurnost postala apsolutno nezaobilazna. Razjasnit ćemo proces naplate plasmana i detaljno analizirati njegovu neraskidivu vezu s kibernetičkom sigurnošću, naglašavajući njezinu ulogu u osiguravanju stabilnosti i uspjeha naplate u digitalnom dobu.

Ključne riječi: bankarsko poslovanje, kibernetička sigurnost, kreditni plasmani

doc. dr. sc. Maja Vretenar Cobović

Sveučilište u Slavonskom Brodu
Odjel društveno-humanističkih znanosti, Odsjek za ekonomiju
ePošta: mvcobovic@unisb.hr

Rođena u Slavonskom Brodu 1984. godine, Maja Vretenar Cobović svoju je akademsku formaciju započela na Ekonomskom fakultetu u Osijeku, gdje je 2008. godine stekla diplomu. Njezina predanost znanstvenom usavršavanju kulminirala je doktoratom iz područja ekonomije u svibnju 2013. godine na Ekonomskom fakultetu Sveučilišta Josipa Jurja Strossmayera u Osijeku. Njezina doktorska disertacija, pod naslovom „Model održivog sustava obveznog i dobrovoljnog mirovinskog osiguranja u Republici Hrvatskoj", svjedoči o njezinu ranom interesu za kompleksna pitanja financija i osiguranja.

Profesionalnu karijeru gradi od 2008. godine na Veleučilištu u Slavonskom Brodu, gdje je svojim radom stekla zvanje profesora stručnog studija. Njezina stručnost i posvećenost akademskoj zajednici prepoznate su i na Sveučilištu u Slavonskom Brodu, gdje od 2020. godine radi kao docentica na Odjelu društveno humanističkih znanosti / Odsjeku za ekonomiju. Osim nastavničkih i istraživačkih obveza, doc.

dr. sc. Vretenar Cobović aktivno doprinosi upravljanju Odjelom obnašajući funkciju zamjenice pročelnika.

Njezina znanstvena znatiželja i analitički pristup ogledaju se u značajnom broju znanstvenih i stručnih radova koje je objavila u polju ekonomije. Kao aktivna članica akademske zajednice, redovito sudjeluje na međunarodnim znanstvenim skupovima, gdje je predstavljala svoje radove i dijelila svoja znanja kao pozvana predavačica. Glavna područja njezina istraživačkog interesa obuhvaćaju monetarne financije, bankarstvo i osiguranje, teme kojima pristupa s dubokim razumijevanjem i analitičkom preciznošću.

Kroz svoju dosadašnju karijeru, doc. dr. sc. Maja Vretenar Cobović pokazuje iznimnu predanost akademskom radu, znanstvenom istraživanju i doprinosu razvoju ekonomske znanosti, aktivno sudjelujući u obrazovanju novih generacija stručnjaka i promičući znanstvenu izvrsnost.

Znanstveno – stručna konferencija

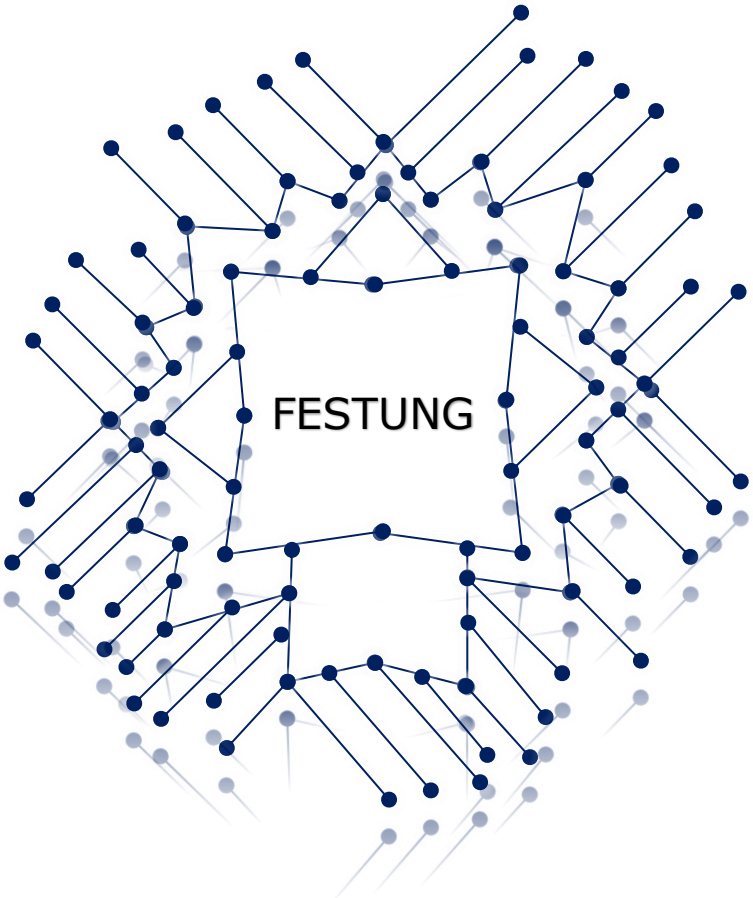
FESTUNG

Slavonski Brod

11. do 13. lipnja 2025. godine

PRISTIGLE PRIJAVE

SAŽETCI



Znanstveno mapiranje i trendovi istraživanja kibernetičke sigurnosti u području ekonomije i menadžmenta

doc. dr. sc. Višnja Bartolović[1], Donata Pospišil, studentica[2], doc. dr. sc. Milan Puvača[3]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Republika Hrvatska, vbartolovic@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, Republika Hrvatska, dpospisil@unisb.hr

[3] doc. dr. sc., Ofir d.o.o. Osijek, Osijek, Republika Hrvatska, milan@ofir.hr

Sažetak: Kibernetička sigurnost u posljednje vrijeme postaje sve važnija tema na sjecištu tehnologije, ekonomije i menadžmenta, no struktura istraživanja u ovom interdisciplinarnom polju nije uvijek jasno definirana. Identificirani trendovi u istraživanju kibernetičke sigurnosti usmjeravaju se prema istraživanju rizika, otpornosti, kriptografiji, blokchain tehnologiji, strojnom učenju i industriji 5.0.

Cilj rada je identificirati istraživačke klastere u području kibernetičke sigurnosti. Obzirom da kibernetička sigurnost značajno korelira s temama ekonomije i menadžmenta provedeno je klasteriranje kibernetičke sigurnosti u području ekonomije i menadžmenta.

Pregledom znanstvenih baza podataka (Web of science) koristeći ključnu temu „cyber security" i njezine inačice identificirano je 28.669 dokumenata te je odabirom područja ekonomije, menadžmenta i poslovanja uzorkovanjem obuhvaćeno 777 istraživanja objavljenih u periodu od 2002. do travnja 2025. godine. U obzir su uzete ključne riječi koje su autori studija eksplicitno navodili te ključne riječi koje Web of Science algoritamski dodaje. Podaci su prethodno pročišćeni i normalizirani, obzirom na različitost znanstvenih područja.

Programom za vizualizaciju VOSviewer, koristeći frakcijsko brojanje za analizu pojavnosti ključnih riječi, identificirani su klasteri znanstvenih istraživanja koji otkrivaju frekvencije, povezanost i intenzitet veza među ključnim temama. Identificirano je devet istraživačkih klastera, najznačajniji autori, institucije, zemlje

te povezanost tema kibernetičke sigurnosti u području ekonomije i menadžmenta s pojedinim ciljevima održivosti Ujedinjenih naroda.

Ključne riječi: kibernetička sigurnost, ekonomija, menadžment, znanstveno mapiranje, analiza ključnih riječi

Scientific mapping and trends in cybersecurity research in the field of economics and management

Abstract: Cybersecurity has recently emerged as a topic of growing significance at the intersection of technology, economics, and management. Key research trends within this domain focus on risk assessment and management, resilience, cryptography, blockchain technology, machine learning, and the implications of Industry 5.0.

The primary objective of this paper is to identify distinct research clusters within the field of cybersecurity. Recognizing the significant interconnections between cybersecurity and the disciplines of economics and management, this study specifically concentrates on mapping the research landscape within this interdisciplinary area through cluster analysis.

A systematic literature search was conducted using the Web of Science Core Collection database, employing the search term "cyber security" and its recognized variants. This initial search yielded 28,669 documents. Subsequent filtering, restricting the selection to the fields of economics, management, and business, resulted in a final sample of 777 publications spanning the period from 2002 to April 2025. The analysis incorporated both author-provided keywords and algorithmically assigned keywords (Keywords Plus) from the Web of Science database. Prior to analysis, the keyword data underwent a rigorous cleaning and normalization process to ensure consistency and accuracy.

Keyword co-occurrence analysis was performed using fractional counting, facilitated by the VOSviewer software. This analysis identified distinct research clusters, revealing the frequency, interconnections, and strength of association between key topics. In total, nine research clusters were delineated. Furthermore, the analysis pinpointed the most influential authors, institutions, and countries contributing to this specific research area. Additionally, the study examined the linkages between the identified cybersecurity research themes within economics and management and specific United Nations Sustainable Development Goals (SDGs).

Keywords: cybersecurity, economics, management, scientific mapping, keyword analysis

Gig ekonomija u Republici Hrvatskoj

doc. dr. sc. Ivona Blažević Dević[1], Marija Rossi, studentica[2]

[1] UNISB, Slavonski Brod, Hrvatska, iblazevic@unisb.hr

[2]UNISB, Slavonski Brod, Hrvatska, mrossi@unisb.hr

Sažetak: Gig ekonomija predstavlja segment ekonomije u kojoj se pojedinci bave obavljanjem kratkoročnih i privremenih poslova. Posao koji žele raditi pronalaze putem raznih platformi gdje se povezuju s klijentima koji trebaju određene usluge. Na taj način pojedinci mogu prihvatiti različite poslove i ponude koje odgovaraju njihovim vještinama. To im omogućuje veću fleksibilnost jer mogu rasporediti posao koji treba obaviti prema vlastitim željama. U empirijskom dijelu rada provedena je anketa među radnicima na području gig ekonomije. Pomoću te ankete testirane su istraživačke pretpostavke te su na temelju njih ekstrahirani zaključci. Cilj rada bio je istražiti i analizirati prednosti i izazove samozapošljavanja u gig ekonomiji u Republici Hrvatskoj, kao i trendove i mogućnosti koje donosi gig ekonomija. U izradi rada korištene su deskriptivne i analitičke metode te kvantitativna metoda za dobivanje podataka u vidu strukturiranog upitnika. Dobiveni podaci obrađeni su deskriptivno statističkom analizom i prikazani uz pomoć grafikona. Rezultati pokazuju kako je jedna od najvećih prednosti gig ekonomije fleksibilnost radnog vremena radnika. Jednako tako, rezultati pokazuju kako će samozapošljavanje u gig ekonomiji nastavit s uzlaznim razvojnim trendom. U zaključku su sumirani rezultati istraživanja te su navedeni prijedlozi za buduća istraživanja.

Ključne riječi: gig ekonomija, samozapošljavanje, digitalne platforme, poduzetništvo

Gig economy in the Republic of Croatia

Abstract: The gig economy represents a segment of the economy in which individuals engage in short-term and temporary jobs. They find the work they want to do through various platforms where they connect with clients who need certain services. In this way, individuals can accept different jobs and offers that match their skills. This allows them greater flexibility as they can schedule the work to be done according to their own preferences. In the empirical part of the work, a survey was conducted among workers in the field of the gig economy. Using this survey, research hypotheses were tested and conclusions were drawn based on them. The aim of the work was to investigate and analyze the advantages and challenges of self-employment in the gig economy in the Republic of Croatia, as well as the trends and opportunities brought by the gig economy. Descriptive and analytical methods and a quantitative method were used to obtain data in the form of a structured questionnaire. The obtained data were processed descriptively by statistical analysis and presented with the help of graphs. The results show that one of the biggest advantages of the gig economy is the flexibility of workers' working hours. Also, the results indicate that technological progress will further increase the number of opportunities for self-employment in the gig economy in the future. The conclusion summarizes the research results and provides suggestions for future research.

Keywords: gig economy, self-employment, digital platforms, entrepreneurship

Prepoznavanje malicioznih napada pomoću strojnog učenja

Antonio Carević, student[1], dr. sc. Mario Dudjak, v. asist.[2]

[1] Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Osijek, Hrvatska, acarevic@etfos.hr

[2]Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Osijek, Hrvatska, mario.dudjak@ferit.hr

Sažetak: U suvremenom, sve složenijem digitalnom okruženju, pravovremeno prepoznavanje malicioznih aktivnosti ključno je za očuvanje sigurnosti informacijskih sustava. Ovaj rad analizira proces učenja klasifikacijskih algoritama na skupovima podataka koji obuhvaćaju različite vrste kibernetičkih napada, s naglaskom na evaluaciju učinkovitosti modela i identifikaciju ključnih faza obrade podataka. Primjenom različitih algoritama strojnog učenja razvijeni su klasifikacijski modeli uz korištenje metoda za odabir značajki i ublažavanje neuravnoteženosti klasa. Rezultati eksperimentalne analize pokazuju da stablo odluke ostvaruje najbolje performanse, dok se SFS omotač i tehnika nasumičnog preuzorkovanja ističu kao najučinkovitije u poboljšanju kvalitete modela. Ovi rezultati naglašavaju važnost pažljivog odabira algoritama i tehnika predobrade podataka. Rad predlaže strukturiran i optimiziran proces klasifikacije s ciljem unaprjeđenja točnosti detekcije malicioznih aktivnosti.

Ključne riječi: klasifikacija, odabir značajki, neuravnotežen skup podataka, strojno učenje, maliciozni napad

Malicious attack detection using machine learning

Abstract: In today's increasingly complex digital environment, timely detection of malicious activities is essential for maintaining the security of information systems. This paper analyzes the learning process of classification algorithms on datasets encompassing various types of cyberattacks, with a particular focus on evaluating model performance and identifying key stages of data processing. By applying a range of machine learning algorithms, classification models were developed using feature selection methods and techniques to address class imbalance. Experimental results demonstrate that decision trees yield the best performance, while the SFS wrapper method and random oversampling technique emerge as the most effective in improving model quality. These findings emphasize the importance of careful algorithm selection and data preprocessing techniques. The paper proposes a structured and optimized classification process aimed at enhancing the accuracy of malicious activity detection.

Keywords: classification, feature selection, imbalanced data set, machine learning, malicious attack

Sigurnosni aspekti daljinskog očitanja brojila električne energije

Maja Čuletić Čondrić, prof. mat. i fiz., pred.[1], Silvio Vilagoš, student[2], Marijana Zarožinski, dipl. ing. mat., asist.[3]

[1]Sveučilište u Slavonskom Brodu, Tehnički odjel, Slavonski Brod, Hrvatska, mccondric@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Tehnički odjel, Slavonski Brod, Hrvatska, svilagos@unisb.hr

[3]Industrijsko-obrtnička škola u Slavonskom Brodu, Slavonski Brod, Hrvatska, marijanazarozinski@gmail.com

Sažetak: Zaštita od kibernetičkih napada na kritičnu infrastrukturu u današnje vrijeme predstavlja prioritet jer se radi o sustavima ključnim za funkcioniranje društva. Na ovom predavanju ćemo istražiti ključne sigurnosne izazove i prijetnje povezane s implementacijom sustava daljinskog očitanja brojila električne energije. Identificirati ćemo potencijalne ranjivosti u komunikacijskim protokolima, infrastrukturi i upravljanju podacima. Cilj rada je analizirati postojeće sigurnosne standarde i preporuke, provesti pregled relevantne literature te identificirati najbolje prakse u osiguravanju povjerljivosti, dostupnosti, te cjelovitosti podataka prikupljenih putem daljinskog očitanja. Metoda uključuje sustavni pregled literature, analizu sigurnosnih protokola i identifikaciju potencijalnih napada. Očekivani rezultat predavanja bi bio sveobuhvatan pregled sigurnosnih rizika i preporuke za jačanje sigurnosti sustava daljinskog očitanja brojila električne energije.

Ključne riječi: daljinsko očitanje, kibernetička sigurnost, zaštita podataka, ranjivosti

Security aspects of remote reading of electricity meters

Abstract: Protection against cyberattacks on critical infrastructure is a priority nowadays, as these are systems that are crucial for the functioning of society. In this lecture, we will explore the key security challenges and threats associated with the implementation of remote meter reading systems. We will identify potential vulnerabilities in communication protocols, infrastructure, and data management. The aim of the paper is to analyze existing security standards and recommendations, conduct a review of relevant literature, and identify best practices in ensuring the confidentiality, availability, and integrity of data collected through remote reading. The method includes a systematic literature review, analysis of security protocols, and identification of potential attacks. The expected outcome of the lecture is be a comprehensive overview of security risks and recommendations for strengthening the security of remote meter reading systems.

Keywords: Remote sensing, cybersecurity, data protection, vulnerabilities

Analiza zapošljavanja i doprinosa ICT sektora BDP-u Europske unije i Republike Hrvatske

doc. dr. sc. Matej Galić[1]

[1] Veleučilište "Lavoslav Ružička" u Vukovaru, Vukovar, Hrvatska, mgalic@vevu.hr

Sažetak: Informacijsko-komunikacijski sektor u današnjoj ekonomiji značajno oblikuje smjer i kretanje gospodarstva. Istražiti će se uloga ICT-a u oblikovanju tržišta rada i doprinos gospodarskom rastu Europske unije i Republike Hrvatske. Glavno istraživanje je fokusirano na broj zaposlenih u ICT sektoru, kretanje zaposlenosti prema vrstama radnih mjesta u ICT-u, ukupan broj zaposlenih i projekcija broja zaposlenih. Sekundarni podaci će se koristiti će se za detaljnu analizu, uključujući Eurostat, Hrvatski zavod za zapošljavanje i European Centre for the Development of Vocational Training. Komparativnom analizom prikazati će se sličnosti i različitosti između podataka na razini EU i Republike Hrvatske. Prikazati će se i utjecaj promjene broja stanovnika na kapacitete rasta ICT sektora. Cilj je prikazati postoji li jasna korelacija između ekonomskog rasta i demografije na razvoj ICT-a, postoje li izazovi u obrazovnoj strukturi na razini EU i Republike Hrvatske te demografsku održivost.

Ključne riječi: demografski trendovi, ekonomski rast, ICT sektor, tržište rada, zaposlenost

Analysis of employment and the contribution of the ICT sector to the GDP of the European Union and the Republic of Croatia

Abstract: The information and communication sector in today's economy significantly shapes the direction and development of the economy. The role of ICT in shaping the labor market and its contribution to economic growth in the European Union and the Republic of Croatia will be investigated. The main research focuses on the number of employees in the ICT sector, employment trends by type of ICT job, the total number of employees and the projection of the number of employees. Secondary data will be used for detailed analysis, including Eurostat, the Croatian Employment Service and the European Centre for the Development of Vocational Training. A comparative analysis will show similarities and differences between data at the EU and Republic of Croatia levels. The impact of population changes on the growth capacity of the ICT sector will also be shown. The aim is to show whether there is a clear correlation between economic growth and demography on the development of ICT, whether there are challenges in the educational structure at the EU and Republic of Croatia levels, and demographic sustainability.

Keywords: demographic trends, economic growth, ICT sector, labor market, employment

Kibernetička sigurnost industrijskih sustava

Mato Galović, dipl. ing. stroj., pred.[1], Ivan Matasović, mag. ing. el., pred.[2], Mato Kokanović, mag. ing. el.[3], Zoran Crnac, dipl. ing. stroj., pred.[4]

[1] Tehnička škola, Slavonski Brod, Republika Hrvatska, mgalovic@unisb.hr

[2]Tehnička škola, Slavonski Brod, Republika Hrvatska, imatasovic@unisb.hr

[3]Tehnička škola, Slavonski Brod, Republika Hrvatska, mkokanovic@unisb.hr

[4]Tehnička škola, Slavonski Brod, Republika Hrvatska, zcrnac2@gmail.com

Sažetak: Industrija 4.0 koristi inteligentnu tehnologiju u cilju povećanja produktivnosti, fleksibilnosti i kvalitete proizvoda te inovativnog razvoja proizvodnih procesa.

Koncept Industrije 4.0 temelji se na inteligentnom umrežavanju strojeva , i drugih proizvodnih sustava koristeći napredne informacijsko-komunikacijske tehnologije. Budući da su sustavi međusobno povezani putem interneta radi razmjene podatka, sigurnost zaštite tih podataka postaje jedan od najvećih izazova u Industriji 4.0. Korištenjem naprednih informacijsko-komunikacijskih tehnologija tvornice postaju sve više izložene kibernetičkim napadima i prijetnjama, čiji je cilj gubitak podataka neophodnih za odvijanje proizvodnih procesa, a posredno i usporavanje procesa proizvodnje, dok u nekim slučajevima rezultiraju oštećenjem opreme koja se koristi.

Cilj ovog rada je upoznavanje s osnovnim aktivnostima i tehnologijama kibernetičke sigurnosti u provođenju koncepta Industrije 4.0. U radu je provedena analiza Europskog izvješća o kibernetičkoj sigurnosti, kao i predložena rješenja zaštite od kibernetičkih napada u industriji.

Detaljnije su objašnjeni oblici kibernetičkih prijetnji, te načini njihovog sprječavanja korištenjem industrijskih sigurnosnih standarda kao što je ISA/IEC 62443.

Ključne riječi: Industrija 4.0, informacijsko-komunikacijske tehnologije, kibernetička sigurnost, sigurnosni standardi

Cyber security of industrial systems

Abstract: Industry 4.0 uses intelligent technology to increase productivity, flexibility and product quality as well as innovative development of production processes.

The Industry 4.0 concept is based on intelligent networking of machines and other production systems using advanced information and communication technologies. Since the systems are interconnected via the Internet for the purpose of data exchange, the security of this data protection becomes one of the biggest challenges in Industry 4.0. By using advanced information and communication technologies, factories are becoming increasingly exposed to cyber attacks and threats, whose goal is the loss of data necessary for the production processes, and indirectly, the slowing down of the production process, while in some cases resulting in damage to the equipment used.

The aim of this paper is to introduce the basic activities and technologies of cybersecurity in the implementation of the Industry 4.0 concept. The paper analyzes the European Cybersecurity Report, as well as proposed solutions for protection against cyber attacks in industry.

The forms of cyber threats are explained in more detail, as well as ways to prevent them using industrial security standards such as ISA/IEC 62443.

Keywords: Industry 4.0, IT - communication technologies, cyber security, security standards

Strojno učenje za detekciju mrežne krađe identiteta analizom URL adresa

doc. dr. sc. Ivana Hartmann Tolić[1], Mirta Vujnovac, mag. educ. math. et inf.[2]

[1] Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Osijek, Hrvatska, ivana.hartmann@ferit.hr

[2]III gimnazija, Osijek, Osijek, Hrvatska, mirta.vujnovac@gmail.com

Sažetak: U posljednji vrijeme phishing napadi, mrežne krađe identiteta, predstavljaju značajnu prijetnju kibernetičke sigurnosti, koristeći lažne web stranice kako bi prevario korisnike u otkrivanju osjetljivih podataka. . Phishing je oblik društvenog inženjeringa u kojem napadači daju pogrešne informacije putem lažnih web stranica kako bi prevarili žrtvu da ustupi osobne podatke radi dobivanja dodatnih informacija ili ostvarivanja financijske koristi. Zbog brzog razvoja tehnologije i taktika krađe identiteta te sve češće razmjene informacija putem interneta, potrebne su učinkovite metode za otkrivanje lažnih URL-ova. Cilj je procijeniti učinkovitost različitih modela u klasifikaciji zlonamjernih i sigurnih web adresa bez analize sadržaja stranica. Ovaj rad daje pregled tradicionalnih algoritama strojnog učenja i modela dubokog učenja za detekciju web stranica za krađu identiteta na temelju URL značajki. Rezultati iz literature potvrđuju da kvalitetna selekcija i obrada značajki, uz primjenu suvremenih modela strojnog učenja, uključujući duboko učenje, znatno poboljšavaju točnost i preciznost detekcije.

Kako se strategije krađe identiteta nastavljaju razvijati, adaptivni modeli poput ensemble tehnika učenja i arhitektura dubokog učenja bit će ključni za zaštitu online sigurnosti te za razumijevanje učinkovitog suzbijanja novonastalih kibernetičkih prijetnji.

Ključne riječi: phishing mrežne stranice, kibernetička sigurnost, strojno učenje, duboko učenje, analiza URL adresa

Machine learning for detecting phishing via URL analysis

Abstract: Phishing attacks have posed a significant threat to cybersecurity in recent years. Phishing is a form of social engineering in which attackers provide misleading information via fake websites in order to trick the victim into disclosing private information in order to obtain further information or gain a financial advantage.

With the rapid development of technology and phishing tactics, as well as access to information and the frequent exchange of information, effective methods for detecting fake URLs are needed. The goal is to evaluate the effectiveness of different models in classifying malicious and legitimate web addresses without analyzing the content of the page.

This paper presents an overview of traditional machine learning algorithms and deep learning models for detecting phishing websites based on URL features.

The results of previous research show that quality selection and processing of URL features in combination with advanced machine learning models, including deep learning models, significantly improve the accuracy and precision of detection.

As phishing strategies continue to evolve, adaptive models such as ensemble learning techniques and deep learning architectures will be fundamental to securing online security and crucial to understanding how to effectively counter emerging cybersecurity threats.

Keywords: phishing websites, cybersecurity, machine learning, deep learning, url analysis

Digitalna dekada i ekonomski rast: Kvantificiranje koristi digitalne transformacije u Europskoj uniji

Tomislav Horvat, mag. oec., pred.[1]

[1] Dilj d.o.o. (članica Nexe grupe), Vinkovci, Hrvatska, thorvatt@gmail.com

Sažetak: Digitalna dekada predstavlja politiku Europske unije za digitalno desetljeće do 2030. godine s ciljem jačanja strateškog okvira za ubrzanje digitalne transformacije do kraja desetljeća. Istražiti će se ekonomske koristi digitalne transformacije analizom ključnih podataka na razini cijele Europske unije i posebno istražiti razina digitalnog razvoja Republike Hrvatske. Korištenjem sekundarnih podataka Europske komisije, Eurostata, Hrvatskog zavoda za zapošljavanje analizirati će se rast BDP-a, udio ICT-a u BDP-u te usporediti s razinom digitalne pismenosti stanovništva i njegovog utjecaja na gospodarstvo. Statističkom analizom će se utvrditi postoji li korelacija između razine digitalizacije i gospodarskog rasta te potencijal Republike Hrvatske za daljnji rast. Cilj rada je utvrditi postoji li jasna poveznica između značajnog rasta BDP-a, razvijenosti zemlje i razvojem ICT sektora, odnosno digitalne pismenosti stanovništva.

Ključne riječi: digitalna dekada, digitalna pismenost, digitalna transformacija, ekonomski rast, ICT sektor

The Digital Decade and Economic Growth: Quantifying the Benefits of Digital Transformation in the European Union

Abstract: The Digital Decade represents the European Union's policy for the Digital Decade by 2030, with the aim of strengthening the strategic framework for accelerating digital transformation by the end of the decade. The economic benefits of digital transformation will be explored by analyzing key data at the level of the entire European Union and, in particular, the level of digital development of the Republic of Croatia. Using secondary data from the European Commission, Eurostat, and the Croatian Employment Service, GDP growth and the share of ICT in GDP will be analyzed and compared with the level of digital literacy of the population and its impact on the economy. Statistical analysis will determine whether there is a correlation between the level of digitalization and economic growth and the potential of the Republic of Croatia for further growth. The aim of the paper is to determine whether there is a clear link between significant GDP growth, the country's development and the development of the ICT sector, i.e. the digital literacy of the population.

Keywords: Digital decade, digital literacy, digital transformation, economic growth, ICT sector

Ekonomska analiza uspješnih mobilnih marketinških kampanja sa naglaskom na sigurnost

Josipa Jakim, studentica[1], doc. dr. sc. Mirko Cobović[2], Jasna Vujčić, prof., v. pred.[3]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, jjakim@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, mcobovic@unisb.hr

[3]Srednja škola Matije Antun Reljković, Slavonski Brod, jasna.vujcic@gmail.com

Sažetak: Rad analizira ekonomsku učinkovitost uspješnih mobilnih marketinških kampanja, stavljajući poseban naglasak na sigurnosne imperativne i dispozicije koje oblikuju njihov razvoj i provedbu. Mobilni marketing, kao dinamičan i sveprisutan oblik promocije, nudi značajne prednosti, no istovremeno nosi i specifične sigurnosne rizike. Cilj ovog istraživanja je identificirati ključne ekonomske faktore koji doprinose uspjehu mobilnih marketinških kampanja te analizirati kako implementacija adekvatnih sigurnosnih mjera i poštivanje zakonske regulative utječu na njihovu dugoročnu održivost.

Istraživanje obuhvaća analizu različitih pristupa mobilnom marketingu, uključujući njihove prednosti i nedostatke, te identificira najčešće sigurnosne rizike s kojima se suočavaju marketinški stručnjaci i korisnici. Nadalje, rad istražuje učinkovitost različitih mjera zaštite u kontekstu mobilnog marketinga te analizira relevantnu zakonsku regulativu i etičke aspekte koji su ključni za izgradnju povjerenja i osiguranje pozitivnog korisničkog iskustva.

Ključne riječi: ekonomska analiza, marketing, mobilni marketing

Economic Analysis of Successful Mobile Marketing Campaigns Focusing on Security

Abstract: This paper analyzes the economic efficiency of successful mobile marketing campaigns, placing a particular emphasis on the security imperatives and dispositions that shape their development and implementation. Mobile marketing, as a dynamic and ubiquitous form of promotion, offers significant advantages, but simultaneously carries specific security risks. The aim of this research is to identify the key economic factors that contribute to the success of mobile marketing campaigns and to analyze how the implementation of adequate security measures and compliance with legal regulations affect their long-term sustainability.

The research encompasses an analysis of various mobile marketing approaches, including their advantages and disadvantages, and identifies the most common security risks faced by marketing professionals and users. Furthermore, the paper investigates the effectiveness of different protection measures in the context of mobile marketing and analyzes the relevant legal regulations and ethical aspects that are crucial for building trust and ensuring a positive user experience.

Keywords: economic analysis, marketing, mobile marketing

O finalnosti i istinitosti interpretacije ponašanja sustava u biologiji i informatici

prof. dr. sc. Franjo Jović[1]

[1] Fakultet elektrotehnike, računarstva i informatičkih tehnologija Osijek, Osijek, Hrvatska, fjovic90@gmail.com

Sažetak: Finalnost je sposobnost ostvarenja cilja organizmičkih sustava. Finalnost je najviša razina informacije. Strojevima je finalnost u načelu usko programirana, kontrolirana i ograničena. Na sučelju strojeva i organizmičkih sustava postavlja se zadatak ispravnog inženjeringa informacije. Zasnovano na radovima Wittgensteina, Schopenhauera i Heideggera predlaže se jednoznačan inženjering informacije u složenim i apstraktnim sustavima poput ciljno orijentirane sportske igre. Razmatra se element ugroze postizanja cilja.

Ključne riječi: samodosljednost, samoodrživost, timski rad, prijetnja

On finality and truthfulness of system behavior interpretation in biology and informatics

Abstract: Finality is the ability of organismic systems to achieve their goals. Finality is the highest level of information. With machines, finality is in principle narrowly programmed, controlled and limited. The task is set for the correct engineering of information at the interface of machines and organismic systems. Based on the works of Wittgenstein, Schopenhauer and Heidegger, it is proposed to unambiguously engineer information in complex and abstract systems such as goal-oriented sports games. The element of jeopardizing the achievement of the goal is considered as well.

Keywords: self-consistency, self-sustainability, teamwork, threat

Učestalost korištenja mobilnog bankarstva u Brodsko-posavskoj županiji

Mirna Jurčević-Ćeranić, studentica[1], Jelena Meštrović, studentica[2], doc. dr. sc. Mirko Cobović[3]

[1] Sveučilište u Slavonskom Brodu, Nova Gradiška, Hrvatska, mirna.jurcevic10@gmail.com

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, mestrovicj307@gmail.com

[3]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, cobovic@unisb.hr

Sažetak: U današnjem digitaliziranom svijetu, u kojem su pametni mobiteli postali neophodan dio svakodnevnih aktivnosti, mobilno bankarstvo predstavlja ključnu inovaciju koja uvelike ubrzava i olakšava financijske poslove. Cilj rada je utvrditi koliko često i za koje usluge korisnici koriste mobilno bankarstvo, identificirati njihove glavne sigurnosne brige te procijeniti razinu povjerenja u sigurnosne mjere koje banke implementiraju. Korištena metoda u istraživanju bila je anketiranje, provedena na 107 ispitanika. Dobiveni rezultati pokazuju visoku razinu prihvaćenosti i redovite upotrebe mobilnog bankarstva. Većina korisnika cijeni praktičnost i brzinu, no postoji oprez prilikom unosa osobnih podataka, a značajan dio neutralan je prema adekvatnosti sigurnosnih mjera banaka. Unatoč tome, velika većina planira nastaviti koristiti mobilno bankarstvo. Rad ističe da je povjerenje u sigurnost ključno za daljnji rast i učestalost korištenja mobilnog bankarstva. Naglašava se potreba za kontinuiranim unaprjeđenjem sigurnosnih protokola, transparentnom komunikacijom banaka o sigurnosnim mjerama i aktivnom edukacijom korisnika kako bi se osiguralo sigurno okruženje i potaknulo još veće povjerenje i korištenje mobilnog bankarstva.

Ključne riječi: bankarstvo, mobilno bankarstvo, rizici, sigurnost, zaštita podataka

Frequency of mobile banking usage in Brod-posavina county

Abstract: In today's digitized world, where smartphones have become an indispensable part of everyday activities, mobile banking represents a key innovation that greatly speeds up and simplifies financial transactions. The aim of this paper is to determine how often and for which services users utilize mobile banking, to identify their main security concerns, and to assess the level of trust in the security measures implemented by banks. The research method used was a survey, conducted on 107 respondents. The results show a high level of acceptance and regular use of mobile banking. Most users appreciate its convenience and speed, but there is caution when entering personal data, and a significant portion is neutral regarding the adequacy of banks' security measures. Despite this, the vast majority plan to continue using mobile banking. The paper emphasizes that trust in security is crucial for the further growth and frequency of mobile banking use. It highlights the need for continuous improvement of security protocols, transparent communication from banks about security measures, and active user education to ensure a secure environment and encourage even greater trust and use of mobile banking.

Keywords: banking, mobile banking, risks, security, data protection

Etika i umjetna inteligencija: ChatGPT, kibernetička sigurnost i privatnost

doc. dr. sc. Matilda Kolić Stanić[1], dr. sc. Marija Lesandrić, v. asist.[2]

[1] Odjel društveno-humanističkih znanosti Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, mkolicstanic@unisb.hr

[2] Odjel društveno-humanističkih znanosti Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, mlesandric@unisb.hr

Sažetak: Primjena generativne umjetne inteligencije zahvatila je brojna područja ljudskih djelatnosti i organizacija, a među brojnim alatima umjetne inteligencije koji su organizacijama na raspolaganju kao pomoć u svakodnevnim poslovnim zadaćama ističe se platforma za interaktivni chat poznata pod nazivom ChatGPT. No ChatGPT donosi sa sobom i neke etičke probleme. Stoga je cilj ovoga rada istražiti etička pitanja koja organizacijama donosi upotreba toga alata s obzirom na sigurnost i privatnost. Premda etički kodeksi umjetne inteligencije ističu da sustavi umjetne inteligencije trebaju biti sigurni i poštivati privatnost korisnika, za sada sigurnost i privatnost nisu dovoljno istražene teme u sve brojnijim istraživanjima o ChatGPT–u. Stoga će ovaj rad pružiti pregled znanstvene literature koja se bavi etičkim pitanjima sigurnosti i privatnosti pri korištenju ChatGPT-a. Glavno istraživačko pitanje na koje ovaj rad želi odgovoriti je: kakve etičke izazove za sigurnost i privatnost donosi primjena ChatGPT-a, najpopularnijeg alata umjetne inteligencije na svijetu.

Ključne riječi: ChatGPT, umjetna inteligencija, etika, kibernetička sigurnost, privatnost

Ethics and Artificial Intelligence: ChatGPT, Cybersecurity and Privacy

Abstract: The application of generative artificial intelligence has affected numerous areas of human activity and organizations, and among the numerous artificial intelligence tools available to organizations to assist in everyday business tasks, the interactive chat platform known as ChatGPT stands out. However, ChatGPT also brings with it some ethical problems. Therefore, the aim of this paper is to explore the ethical issues that the use of this tool brings to organizations with regard to security and privacy. Although AI ethical codes emphasize that AI systems should be secure and respect user privacy, security and privacy are currently not sufficiently explored topics in the increasing number of research studies on ChatGPT. This paper will therefore provide an overview of the scientific literature that addresses ethical issues of security and privacy when using ChatGPT. The main research question that this paper seeks to answer is: what ethical challenges for security and privacy does the application of ChatGPT – the most popular artificial intelligence tool in the world – bring.

Keywords: ChatGPT, artificial intelligence, ethics, cybersecurity, privacy

Marketinške strategije i sigurnosni izazovi u fazi lansiranja digitalnog bankarskog proizvoda

Mirjana Kraljević, studentica[1], doc. dr. sc. Andreja Katolik Kovačević[2]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, mkraljevic@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, akkovacevic@unisb.hr

Sažetak: Digitalni marketinški proizvodi, s posebnim naglaskom na bankarske proizvode i mobilne aplikacije banaka za osobne financije, predstavljaju ključan segment suvremenog tržišta, pružajući korisnicima jednostavniji pristup financijskim uslugama uz visoku razinu sigurnosti. Cilj rada je analizirati marketinške strategije i sigurnosne izazove u fazi uvođenja digitalnog bankarskog proizvoda, s naglaskom na mobilnu aplikaciju Addiko banke. Kroz studiju slučaja istražit će se koje strategije banka koristi za promociju i privlačenje korisnika, kako se aplikacija pozicionira na tržištu te koliko su te strategije učinkovite. Osim toga, rad će ispitati kako se mobilna aplikacija navedene banke ističe i razlikuje od sličnih proizvoda konkurencije na tržištu. Aktualni trendovi korištenja mobilnog bankarstva prema podacima Hrvatske narodne banke u stalnom su porastu. U 2022. godini 39% potrošača u Republici Hrvatskoj imalo je ugovorenu uslugu internetskog bankarstva, dok je 53% potrošača koristilo mobilno bankarstvo. Ovaj rad proizašao je iz završnog rada studentice Sveučilišta u Slavonskom Brodu.

Ključne riječi: marketinške strategije, sigurnost, digitalni proizvodi

Marketing strategies and security challenges in the launch phase of a digital banking product

Abstract: Digital marketing products, with a particular focus on banking products and mobile banking applications for personal finance, represent a key segment of the modern market, providing users with easier access to financial services along with a high level of security. The aim of this paper is to analyze marketing strategies and security challenges during the introduction phase of a digital banking product, with a focus on the mobile application of Addiko Bank. Through a case study, the paper will explore which strategies the bank employs to promote and attract users, how the application is positioned in the market, and how effective these strategies are. Furthermore, the paper will examine how the bank's mobile application stands out and differs from similar competitive products in the market. Current trends in the use of mobile banking, according to data from the Croatian National Bank, are continuously increasing. In 2022, 39% of consumers in the Republic of Croatia had contracted internet banking services, while 53% used mobile banking. This paper has emerged from the final thesis of a student at the University of Slavonski Brod.

Keywords: marketing strategies, security, digital products

Razvoj pametnih gradova

doc. dr. sc. Anita Kulaš Mirosavljević[1], Valentina Vuleta, studentica[2]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, akmirosavljevic@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, vvuleta@unisb.hr

Sažetak: U posljednjih nekoliko godina pametni gradovi postali su svjetski fenomen s različitim oblicima koji se pojavljuju u različitim dijelovima svijeta. Pametni grad se obično definira kao metropolitansko područje koje primjenom moderne tehnologije omogućuje veću kvalitetu života svojim stanovnicima. Njegov glavni cilj je poboljšati urbani život korištenjem informacijske tehnologije u pogledu prometa, sigurnosti, energije, otpada, pa čak i zdravstvenih usluga. Svrha rada je istražiti na koji način funkcioniraju pametni gradovi i kako dolaze do podataka. Cilj rada je istražiti koliko su građanima jasne dobrobiti pametnih gradova te prednosti digitalnih tehnologija. Ovo istraživanje temelji se na kvalitativnoj i deskriptivnoj metodologiji, s fokusom na analizu sekundarnih podataka. Pristup uključuje pregled relevantne znanstvene i stručne literature, strateških dokumenata Europske unije, nacionalnih razvojnih strategija te javno dostupnih izvješća vezanih uz razvoj pametnih gradova. Glavni izvori podataka uključuju dokumente politike EU-a, akademske članke, institucionalna izvješća i provjerene internetske platforme. Rezultati su pokazali da je kombinacija digitalnih tehnologija s urbanom infrastrukturom povećala stupanj ovisnosti pametnih gradova o ogromnim količinama podataka prikupljenih od građana, senzora i drugih digitalnih sustava. Rad je omogućio predstavljanje svih izazova i perspektiva razvoja pametnih gradova, opisujući izazove financiranja i održavanja pametnih gradova, sigurnost podataka i zaštita privatnosti, društvene izazove i digitalnu uključenost te buduće tehnologije u razvoju pametnih gradova.

Ključne riječi: razvoj, sigurnost, pametni gradovi

Development of smart cities

Abstract: In recent years, smart cities have become a global phenomenon with different forms appearing in different parts of the world. A smart city is usually defined as a metropolitan area that, through the application of modern technology, enables a higher quality of life for its inhabitants. Its main goal is to improve urban life by using information technology in terms of traffic, security, energy, waste, and even health services. The purpose of the paper is to investigate how smart cities work and how they obtain data. The aim of the paper is to investigate how citizens understand the benefits of smart cities and the advantages of digital technologies. This research is based on a qualitative and descriptive methodology, with a focus on secondary data analysis. The approach includes a review of relevant scientific and professional literature, strategic documents of the European Union, national development strategies, and publicly available reports related to the development of smart cities. The main sources of data include EU policy documents, academic articles, institutional reports, and verified online platforms. The results showed that the combination of digital technologies with urban infrastructure has increased the degree of dependence of smart cities on huge amounts of data collected from citizens, sensors and other digital systems. The work enabled the presentation of all the challenges and perspectives of smart city development, describing the challenges of financing and maintaining smart cities, data security and privacy protection, social challenges and digital inclusion, and future technologies in the development of smart cities.

Keywords: development, security, smart cities

Etičnost na društvenim mrežama

doc. dr. sc. Anita Kulaš Mirosavljević[1], Nikolina Matić, studentica[2], dr. sc. Branka Martić, pred.[3]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, akmirosavljevic@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska,

[3]Brodsko-posavska županija, Slavonski Brod, Hrvatska,

Sažetak: Društvene mreže su postale sastavni dio suvremenog života, revolucionirajući način na koji se komunicira, dijele informacije te formiraju odnosi. Svrha i cilj rada je istražiti duboki utjecaj društvenih mreža na etičke norme, ispitujući kako platforme poput Facebooka, Instagrama, YouTubea, oblikuju moralno ponašanje i stavove pojedinaca. Stoga je nužna analiza različitih etičkih dilema koje proizlaze iz korištenja društvenih mreža, uključujući pitanja privatnosti, dezinformacija, govora mržnje i cyberbullyinga. Posebna pažnja je posvećena ulozi kibernetičke sigurnosti u kontekstu etičkog ponašanja na društvenim mrežama. U radu su korištene deskriptivna metoda, kvantitativna metoda, induktivna metoda, anketa i metoda analize i sinteze. Rezultati istraživanja kojima je cilj bio ispitati utjecaj društvenih mreža na etičke norme s naglaskom na ulogu kibernetičke sigurnosti pokazali su raznolike rezultate. U prosjeku, ispitanici se nisu susreli sa povredom osobnih podataka, ali niti jesu niti nisu uvjereni u prepoznavanje pokušaja prevare na internetu te nisu sigurni u svoju informiranost o kibernetičkoj sigurnosti. Rad je doprinio saznanju da se ljudi trebaju dodatno educirati o važnosti kibernetičke sigurnosti kako bi znali prepoznati prijetnje s kojima će se nekada susresti.

Ključne riječi: kibernetička sigurnost, etika, društvena mreža

Ethics on social networks

Abstract: Social networks have become an integral part of modern life, revolutionizing the way we communicate, share information, and form relationships. The purpose and goal of the paper is to explore the profound influence of social networks on ethical norms, examining how platforms such as Facebook, Instagram, and YouTube shape the moral behavior and attitudes of individuals. Therefore, it is necessary to analyze various ethical dilemmas that arise from the use of social networks, including issues of privacy, disinformation, hate speech, and cyberbullying. Special attention is paid to the role of cybersecurity in the context of ethical behavior on social networks. The paper uses descriptive methods, quantitative methods, inductive methods, surveys, and methods of analysis and synthesis. The results of the research aimed at examining the influence of social networks on ethical norms with an emphasis on the role of cybersecurity showed diverse results. On average, respondents did not encounter a breach of personal data, but they were neither convinced nor unconvinced of recognizing fraud attempts on the Internet, and they were not confident in their information about cybersecurity. The work contributed to the realization that people need to be further educated about the importance of cybersecurity so that they can recognize the threats they will someday encounter.

Keywords: cybersecurity, ethics, social network

Provjera znanja o kibernetičkoj sigurnosti u srednjim školama pomoću digitalnog kviza

Ivana Lovrić Senjak, studentica[1], doc. dr. sc. Mirko Cobović[2], Žaklina Bender, prof.[3], Anita Barišić, dipl. pead.[4]

[1] Sveučilište Slavonski Brod, Slavonski Brod, Hrvatska, ilovricsenjak@unisb.hr

[2]Sveučilište Slavonski Brod, Slavonski Brod, Hrvatska, mcobovic@unisb.hr

[3]Gimnazija Požega, Požega, Hrvatska, ecce.homo.zb@gmail.com

[4]Gimnazija "Matija Mesić" Slavonski Brod, Slavonski Brod, Hrvatska, anitaorec2@gmail.com

Sažetak: Ovaj rad istražuje razinu znanja srednjoškolaca o osnovama kibernetičke sigurnosti putem digitalnog kviza. Cilj je bio identificirati područja dobre informiranosti i ona koja zahtijevaju dodatnu edukaciju. U kvizu je sudjelovalo 268 učenika iz triju gimnazija. Rezultati pokazuju visoku ukupnu točnost (87,69 %), s najboljim rezultatima u temama lozinki i digitalnog traga te najslabijima u prepoznavanju osobnih podataka, ransomwarea i 2FA. Nije utvrđena značajna povezanost između točnosti i vremena rješavanja niti između uređaja i uspješnosti. Rad ističe važnost strukturirane edukacije o kibernetičkoj sigurnosti.

Ključne riječi: kibernetička sigurnost, digitalna provjera, obrazovno mjerenje, gimnazije, statistička analiza

Assessing cybersecurity knowledge among high school students using a digital quiz

Abstract: This paper examines the level of cybersecurity knowledge among high school students using a digital quiz as an assessment tool. The objective was to identify areas of strong awareness as well as topics requiring further educational support. A total of 268 students from three grammar schools participated in the quiz. The results indicate a high overall accuracy rate (87.69%), with the highest performance observed in topics related to password security and digital footprints, and the lowest in identifying personal data, ransomware, and two-factor authentication (2FA). No statistically significant correlations were found between accuracy and time taken nor between device type and performance. The findings underscore the importance of structured cybersecurity education in secondary schools.

Keywords: Cybersecurity, Digital assessment, Educational measurement, Grammar schools, Statistical analysis

Ozbiljne igre o kibernetičkoj sigurnosti u kurikuluma nastave informatike

Ivana Lovrić Senjak, studentica[1], Slavko Dukarić[2], Mihovil Gašić, student[3]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, ilovricsenjak@unisb.hr

[2]Ministarstvo obrane Republike Hrvatske MORH, Zagreb, Hrvatska, slavko.dukaric@morh.hr

[3]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, mgasic@unisb.hr

Sažetak: Ovaj rad analizira mogućnosti implementacije ozbiljnih igara o kibernetičkoj sigurnosti u nastavi informatike te njihovu integraciju u kurikulum osnovnoškolskih i gimnazijskih programa. Primijenjen je kvalitativni pristup i deskriptivna evaluacija osam web-baziranih igara, uz mapiranje njihovih sadržaja na ishode iz važećeg kurikuluma. Rezultati pokazuju da postoji određeni prostor za usklađivanje sadržaja igara s predviđenim ishodima učenja, iako su uočena i ograničenja unutar kurikularne strukture. Ozbiljne igre prepoznate su kao vrijedan alat za suvremeno planiranje i unapređenje nastave informatike.

Ključne riječi: kibernetička sigurnost, gamifikacija, informatika, kurikulum, ozbiljne igre

Serious games on cybersecurity in the computer science curriculum

Abstract: This paper analyzes the possibilities for implementing serious games on cybersecurity in computer science education and their integration into the curriculum of primary and secondary school programs. A qualitative approach and descriptive evaluation of eight web-based games were applied, mapping their content to the learning outcomes prescribed by the current curriculum. The results indicate that there is some potential for aligning the games' content with the expected learning outcomes, although certain limitations within the curricular structure were identified. Serious games are recognized as a valuable tool for modern planning and enhancement of computer science education.

Keywords: cybersecurity, gamification, informatics, curriculum, serious games

Sigurnosni izazovi IoT uređaja

Ivan Matasović, mag. ing. el., pred.[1], Mato Kokanović, mag. ing. el., pred.[2], Mato Galović, dipl. ing. stroj., pred.[3], Zoran Crnac, dipl. ing. el., pred.[4]

[1] Tehnička škola Slavonski Brod, Slavonski Brod, Hrvatska, imatasovic@unisb.hr

[2]Tehnička škola Slavonski Brod, Slavonski Brod, Hrvatska, mkokanovic@unisb.hr

[3]Tehnička škola Slavonski Brod, Slavonski Brod, Hrvatska, mgalovic@unisb.hr

[4]Tehnička škola Slavonski Brod, Slavonski Brod, Hrvatska, zcrnac@unisb.hr

Sažetak: Internet stvari (IoT) predstavlja sveprisutnu tehnologiju modernog doba koja omogućuje međusobnu komunikaciju uređaja i razmjenu podataka putem interneta. S obzirom na sve širu primjenu u pametnim kućama, industriji i kritičnoj infrastrukturi, sigurnost IoT uređaja postaje ključno pitanje. Zbog svoje povezanosti i često nedovoljne razine zaštite, IoT uređaji predstavljaju značajnu metu za različite oblike kibernetičkih napada.

Cilj ovog rada je analizirati osnovne prijetnje koje se odnose na sigurnost IoT uređaja, identificirati ranjivosti, te prikazati moguće metode zaštite i dobre prakse u području kibernetičke sigurnosti. U sklopu praktičnog dijela rada provedeno je testiranje sigurnosti jedne pametne WiFi kamere, kako bi se kroz konkretan primjer pokazale potencijalne slabosti i načini zaštite.

Rad donosi pregled aktualnih sigurnosnih prijetnji, metode sigurnosnog testiranja, kao i prijedloge tehničkih i organizacijskih mjera zaštite u skladu s relevantnim sigurnosnim standardima.

Ključne riječi: Internet stvari (IoT), kibernetička sigurnost, WiFi kamera, ranjivosti, testiranje sigurnosti

Security Challenges of IoT Devices

Abstract: The Internet of Things (IoT) represents a ubiquitous modern technology that enables communication between devices and the exchange of data via the internet. Given its widespread use in smart homes, industry, and critical infrastructure, the security of IoT devices has become a key concern. Due to their connectivity and often insufficient levels of protection, IoT devices are a significant target for various forms of cyberattacks.

The aim of this paper is to analyze the main threats related to the security of IoT devices, identify vulnerabilities, and present possible protection methods and best practices in the field of cybersecurity. As part of the practical section, a security test was conducted on a smart WiFi camera to demonstrate potential weaknesses and methods of protection through a concrete example.

This paper provides an overview of current security threats, methods of security testing, and offers proposals for technical and organizational protection measures in accordance with relevant security standards.

Keywords: Internet of Things (IoT), cybersecurity, WiFi camera, vulnerabilities, security testing

Čuvari virtualnog praga: Suočavanje s kibernetičkim prijetnjama u virtualnom turizmu

doc. dr. sc. Igor Mavrin[1]

[1] Akademija za umjetnost i kulturu u Osijeku, Osijek, Republika Hrvatska, imavrin@gmail.com

Sažetak: Uspon virtualnog turizma, pokretan umjetnom inteligencijom (UI), virtualnom stvarnosti (VR), proširenom stvarnosti (AR) i algoritamima strojnog učenja, transformira turističko iskustvo pružajući imerzivne, personalizirane i održive alternative fizičkom putovanju. Međutim, ova transformacija također otvara novo područje kibernetičkih prijetnji. Budući da AI-personalizacija prikuplja velike količine korisničkih podataka, a VR sustavi zahtijevaju stalnu provjeru identiteta i prijenos podataka, virtualni turizam postaje ranjiv na kibernetičke napade, uključujući krađu identiteta, curenje podataka i deepfake imitacije.

Za zaštitu ovih okruženja predlažu se decentralizirani sustavi identiteta poput Self-Sovereign Identity (SSI), metode enkripcije (AES, RSA, ECC) i autentikacija temeljena na blockchain tehnologiji. Osim toga, višeslojni sigurnosni modeli i praćenje u stvarnom vremenu poboljšavaju sposobnosti otkrivanja prijetnji. Unatoč ovim naprecima, izazovi poput nedostatka standardizacije, visokih troškova implementacije i stalno promjenjivog okruženja prijetnji i dalje postoje. Etička pitanja vezana uz utjecaj AI-ja na privatnost i identitet dodatno kompliciraju raspravu o kibernetičkoj sigurnosti.

Ovaj rad istražuje sjecište kibernetičke sigurnosti i virtualnog turizma, naglašavajući hitnu potrebu za adaptivnim okvirima koji štite integritet korisnika bez narušavanja imerzivnog iskustva. Poziva se na interdisciplinarnu suradnju u razvoju sigurnih, etičkih i inkluzivnih digitalnih turističkih ekosustava.

Ključne riječi: virtualni turizam, kibernetička sigurnost, umjetna inteligencija (AI), zaštita podataka, prijetnje deepfake sadržajem

Guardians of the virtual gateway: Addressing cybersecurity threats in virtual tourism

Abstract: The rise of virtual tourism, powered by AI technologies, virtual reality (VR), augmented reality (AR), and machine learning, transforms the travel experience by offering immersive, personalised, and sustainable alternatives to physical travel. However, this transformation also introduces a new frontier of cybersecurity threats. With AI-driven personalisation collecting vast amounts of user data, and VR systems requiring continuous identity verification and data transmission, virtual tourism becomes vulnerable to cyber attacks, including identity theft, data breaches, and deepfake impersonation.

Decentralised identity frameworks like Self-Sovereign Identity (SSI), encryption techniques (AES, RSA, ECC), and blockchain-based authentication are proposed to secure these environments. Additionally, layered defence models and real-time monitoring enhance threat detection capabilities. Despite these advancements, challenges such as standardisation gaps, high implementation costs, and the evolving threat landscape remain. Ethical concerns around AI's impact on privacy and identity further complicate the cybersecurity discourse.

This paper explores the intersection of cybersecurity and virtual tourism, emphasising the urgent need for adaptive frameworks that safeguard user integrity without compromising immersive experiences. It calls for interdisciplinary collaboration to develop secure, ethical, and inclusive digital travel ecosystems.

Keywords: Virtual Tourism; Cybersecurity; Artificial Intelligence (AI); Data Privacy; Deepfake Threats

Fiskalizacija 2.0: pravni okvir, digitalna transformacija i učinci na mikro i male poduzetnike u Republici Hrvatskoj

doc. dr. sc. Ivana Miklošević[1]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, imiklosevic@unisb.hr

Sažetak: Rad predstavlja pravno-ekonomsku analizu Prijedloga Zakona o fiskalizaciji iz 2025. godine, razvijenog u okviru reforme Fiskalizacija 2.0, kojim se uvodi obvezna fiskalizacija računa u B2C, B2B i B2G segmentima, obvezno korištenje eRačuna, digitalni model izvještavanja te aplikacija MIKROeRAČUN namijenjena malim poreznim obveznicima. Cilj istraživanja je evaluirati regulatorne promjene, identificirati ključne izazove u provedbi te sagledati moguće učinke na poslovanje, s naglaskom na mikro i male poduzetnike.

Empirijski dio temelji se na kvalitativnoj analizi deset polustrukturiranih intervjua s poduzetnicima iz različitih sektora. Podaci su analizirani tematski i dopunjeni deskriptivnim prikazom učestalosti odgovora. Osam poduzetnika navelo je složenost digitalne prilagodbe kao glavni izazov, sedam poduzetnika istaknulo je početne troškove implementacije novog sustava, dok ih je šest prepoznalo koristi poput povećane transparentnosti i smanjenja administrativnih opterećenja.

Zaključci ukazuju na potrebu za jačanjem institucionalne podrške, provedbenih smjernica i edukativnih alata kako bi se omogućila učinkovita primjena zakona u skladu s ciljevima digitalne tranzicije i fiskalne transparentnosti.

Ključne riječi: Fiskalizacija 2.0, digitalna fiskalizacija 2.0, e-Račun, mikro i mala poduzeća u procesu digitalne fiskalizacije

Fiscalization 2.0: legal framework, digital transformation and impacts on micro and small enterprises in the Republic of Croatia

Abstract: This paper presents a legal and economic analysis of the Draft Fiscalization Act of 2025, developed within the framework of the Fiscalization 2.0 reform. The Act introduces mandatory fiscalization of invoices in the B2C, B2B, and B2G segments, the compulsory use of e-Invoices, a digital reporting model, and the MIKROeRAČUN application designed for small taxpayers. The aim of the research is to evaluate regulatory changes, identify key implementation challenges, and assess the potential impacts on business operations, with a particular focus on micro and small enterprises.

The empirical part of the research is based on a qualitative analysis of ten semi-structured interviews conducted with entrepreneurs from different sectors. The collected data were analysed thematically and supplemented with a descriptive statistical presentation of response frequencies. Eight entrepreneurs identified the complexity of digital adaptation as the main challenge, seven highlighted the initial costs of implementing the new system, while six recognized benefits such as increased transparency and reduced administrative burdens.

The findings emphasize the need to strengthen institutional support, provide detailed implementation guidelines, and develop educational tools to ensure the effective application of the Act in line with the goals of digital transformation and fiscal transparency.

Keywords: Fiscalization 2.0, Digital Fiscalization 2.0, e-Invoice, Micro and Small Enterprises in the Process of Digital Fiscalization

Umjetna inteligencija i kibernetička sigurnost: Stavovi zaposlenika i izazovi za suvremena poduzeća

doc. dr. sc. Ivana Miklošević[1], Gabrijela Bosak, studentica[2]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, imiklosevic@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, gbosak@unisb.hr

Sažetak: Rad analizira primjenu umjetne inteligencije u suvremenom poslovnom okruženju, s naglaskom na njezin utjecaj na digitalnu transformaciju, kibernetičku sigurnost i konkurentnost poduzeća. Cilj istraživanja bio je ispitati percepcije zaposlenika o mogućnostima, rizicima i izazovima povezanim s implementacijom umjetne inteligencije u organizacijske procese. Istraživanje je provedeno metodom anketiranja na uzorku od 111 ispitanika, a podaci su obrađeni deskriptivnom statistikom.

Rezultati pokazuju da ispitanici umjetnu inteligenciju najčešće povezuju s analitikom podataka, automatizacijom poslovanja, marketingom i kibernetičkom sigurnošću. Kao najveće koristi ističu se optimizacija procesa i brže donošenje odluka, dok se kao ključni izazovi navode gubitak radnih mjesta, nedostatak stručnog kadra, etička pitanja i zaštita privatnosti. Većina ispitanika smatra da njihovi poslodavci ne ulažu dovoljno u kibernetičku sigurnost te podržavaju snažniju regulaciju primjene umjetne inteligencije.

Zaključno, umjetna inteligencija predstavlja važan čimbenik održivog razvoja i digitalne otpornosti poduzeća, ali zahtijeva odgovornu implementaciju, razvoj sigurnosnih protokola te kontinuirano jačanje digitalnih kompetencija zaposlenika.

Ključne riječi: digitalna transformacija, implementacija umjetne inteligencije, kibernetička sigurnost, poslovno okruženje, umjetna inteligencija, zaposlenici

Artificial intelligence and cybersecurity: employee perspectives and challenges for modern enterprises

Abstract: This paper examines the application of artificial intelligence (AI) in the contemporary business environment, with a particular focus on its impact on digital transformation, cybersecurity, and enterprise competitiveness. The objective of the research was to explore employees' perceptions regarding the opportunities, risks, and challenges associated with the implementation of AI in organisational processes. The research was conducted using a survey method on a sample of 111 respondents, and the collected data were analysed using descriptive statistics.

The results indicate that respondents most commonly associate AI with data analytics, business process automation, marketing, and cybersecurity. The most frequently recognised benefits include process optimisation and faster decision-making, while key concerns are related to job displacement, shortage of skilled personnel, ethical considerations, and data privacy. A majority of respondents believe that their employers do not invest sufficiently in cybersecurity and express support for stronger regulation of AI usage.

In conclusion, artificial intelligence is emerging as a key enabler of sustainable development and digital resilience in enterprises. However, its effective implementation requires responsible governance, the development of security protocols, and the continuous strengthening of employees' digital competencies.

Keywords: digital transformation, implementation of artificial intelligence, cybersecurity, business environment, artificial intelligence, employees

Kibernetička sigurnost kao poslovna prednost: Ekonomika primjene UI sustava u nadzoru i upravljanju rizicima

doc. dr. sc. Sanela Ravlić[1]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, sravlic@unisb.hr

Sažetak: U eri sve veće digitalizacije poslovanja, kibernetička sigurnost više nije isključivo tehničko pitanje, već postaje strateški poslovni resurs. Ovo predavanje bavi se ekonomskim aspektima primjene inteligentnih sigurnosnih sustava, s fokusom na Mogen – UI sustav za automatiziranu video analitiku i upravljanje incidentima.

Cilj rada jest predstavljanje konkretnih primjera njihove primjene u maloprodaji, uredskim zgradama i industriji, uključujući automatsko prepoznavanje sumnjivih radnji, optimizaciju korištenja prostora, kontrolu pristupa te upravljanje sigurnosnim incidentima u realnom vremenu. Predstavit će se uvid u prednosti SaaS modela (softver kao usluga), kroz koji se omogućuje fleksibilna i skalabilna primjena sigurnosne tehnologije bez velikih početnih ulaganja, čime se otvaraju nove mogućnosti za tvrtke svih veličina.

Ključne riječi: kibernetička sigurnost, umjetna inteligencija

Cybersecurity as a Business Advantage: The Economics of AI-Based Surveillance and Risk Management Systems

Abstract: In an era of increasing business digitalization, cybersecurity is no longer merely a technical issue—it has become a strategic business resource. This presentation focuses on the economic aspects of implementing intelligent security systems, with particular emphasis on Mogen, AI system for automated video analytics and incident management.

The aim of this work is to present concrete examples of their application in retail, office buildings, and industrial environments, including automated detection of suspicious activities, space utilization optimization, access control, and real-time security incident management. The presentation will also provide insights into the advantages of the SaaS (Software as a Service) model, which enables flexible and scalable use of security technology without substantial initial investments, thereby creating new opportunities for companies of all sizes.

Keywords: cybersecurity, artificial intelligence

Uloga kibernetičke sigurnosti u jačanju regionalne gospodarske otpornosti: Institucionalne i geopolitičke perspektive

doc. dr. sc. Sanela Ravlić[1], dr. sc. Ivana Unukić, v. asist.[2]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, sravlic@unisb.hr

[2] Ekonomski fakultet u Osijeku, Osijek, Hrvatska, ivana.unukic@efos.hr

Sažetak: Ovaj rad istražuje ulogu sigurnosti i kibernetičke sigurnosti unutar šire analize regionalne ekonomije jugoistočne Europe, s fokusom na geopolitičke i društvene izazove koji oblikuju gospodarske procese u Hrvatskoj i susjednim zemljama. U digitaliziranom gospodarstvu, sigurnosna infrastruktura – uključujući zaštitu informacijskih sustava, podataka i komunikacijskih kanala – postaje ključan preduvjet za održivi regionalni razvoj, gospodarsku stabilnost i prekograničnu suradnju.

Kibernetička sigurnost razmatra se ne samo kao tehnički zahtjev, već i kao element koji je duboko povezan s institucionalnim kapacitetima sigurnosnih protokola i razinom međusobnog povjerenja među državama regije. Jezične barijere dodatno otežavaju usklađivanje sigurnosnih mjera i krizne komunikacije, čime se povećava rizik od digitalne fragmentacije prostora koji teži integraciji.

U radu se analizira kako različite razine kibernetičke otpornosti i sigurnosne politike među državama utječu na investicijsku atraktivnost, inovacijsku suradnju i digitalnu transformaciju unutar regije. Rad nudi interdisciplinarni pristup koji spaja ekonomske, sigurnosne, jezične i tehnološke perspektive, s ciljem oblikovanja preporuka za stvaranje otpornije i sigurnije regionalne gospodarske arhitekture.

Ključne riječi: kibernetička sigurnost, regionalni razvoj, geopolitička stabilnost

The Role of Cybersecurity in Strengthening Regional Economic Resilience: Institutional and Geopolitical Perspectives

Abstract: This paper explores the role of security and cybersecurity within a broader analysis of the regional economy of Southeast Europe, with a focus on the geopolitical and societal challenges that shape economic processes in Croatia and neighboring countries. In an increasingly digitalized economy, security infrastructure—including the protection of information systems, data, and communication channels—has become a key prerequisite for sustainable regional development, economic stability, and cross-border cooperation.

Cybersecurity is examined not only as a technical requirement, but also as an element closely linked to institutional capacities, security protocols, and the level of mutual trust among countries in the region. Language barriers further complicate the harmonization of security measures and crisis communication, increasing the risk of digital fragmentation within a space striving for integration.

The paper analyzes how varying levels of cyber resilience and security policies among countries affect investment attractiveness, innovation collaboration, and digital transformation across the region. An interdisciplinary approach is applied, combining economic, security, linguistic, and technological perspectives, with the aim of formulating recommendations for building a more resilient and secure regional economic architecture.

Keywords: cybersecurity, regional development, geopolitical stability

Izgradnja otpornosti poduzeća s osvrtom na poslovne krize u digitalnom dobu

doc. dr. sc. Lena Sigurnjak[1], doc. dr. sc. Sanja Knežević Kušljić[2], Ivana Sluganović, studentica[3]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, lsigurnjak@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, sknezevic@unisb.hr

[3]Sveučilište u Slavonskom Brodu- student, Slavonski Brod, Hrvatska, isluganovic@unisb.hr

Sažetak: Radom se analizira otpornost poduzeća s posebnim naglaskom na poslovne krize u digitalnom dobu. Suočena s nepredvidivim i promjenjivim okruženjem, poduzeća moraju razviti otpornost kako bi se prilagodila tržišnim promjenama i očuvala stabilnost. Teorijski okvir poslovne krize u digitalnom dobu uključuje analizu različitih vrsta poslovnih kriza, jer su krizne situacije jedan od glavnih pokretača neravnoteže na tržištu. Stoga, svrha rada je istaknuti potrebu da poduzeća moraju adekvatno prilagoditi svoje poslovne strategije kako bi uspješno odgovorila na krizu u kojoj su se našla. Za kvalitetnu prilagodbu kriznim situacijama važno je na vrijeme uočiti problem te razviti poslovne strategije za rješavanje istog. Cilj rada je detaljno obrazložiti opasnosti koje poslovne krize mogu donijeti poduzećima te način na koji digitalizacija poslovanja može utjecati na nastanak krize kao i upravljanje istom. Digitalizacija je sve zastupljenija u poduzećima zbog brojnih prednosti koje donosi poslovanju, stoga je za izgradnju otpornosti poduzeća izuzetno važno uvođenje tehnoloških rješenja i inovacija. U radu se koriste metode analize, sinteze, indukcije, dedukcije, te deskriptivna metoda za prikaz istraženih pojmova. U istraživačkom djelu rada se provodi istraživanje putem ankete provedeno među 60 ispitanika, a kojim se nastoji istaknuti važnost kibernetičke sigurnosti u digitalnom poslovanju te načine na koje se ona može ostvariti.

Ključne riječi: otpornost, poslovna kriza, digitalizacija, kibernetička sigurnost, tehnologija

Building corporate resilience with a focus on business crises in the digital age

Abstract: The paper analyzes corporate resilience with a special emphasis on business crises in the digital age. Faced with an unpredictable and changing environment, companies must develop resilience in order to adapt to market changes and maintain stability. The theoretical framework of business crises in the digital age includes an analysis of various types of business crises, as crisis situations are one of the main drivers of market imbalance. Therefore, the purpose of the paper is to emphasize the need for companies to adequately adapt their business strategies in order to successfully respond to crises they encounter. For quality adaptation to crisis situations, it is important to identify problems in time and develop business strategies to solve them. The aim of the paper is to explain in detail the dangers that business crises can bring to companies and the ways in which business digitalization can affect the emergence of a crisis as well as its management. Digitization is increasingly common in companies due to the numerous advantages it brings to business; therefore, the introduction of technological solutions and innovations is extremely important for building corporate resilience. The paper uses methods of analysis, synthesis, induction, deduction, and a descriptive method to present the researched concepts. In the research part of the paper, a survey was conducted among 60 respondents, aiming to highlight the importance of cyber security in digital business and the ways in which it can be achieved.

Keywords: resilience, business crisis, digitization, cyber security, technology

Modularna, performativna multimedijska umjetnost

doc. dr. sc. Vesna Srnić[1]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, vsrnic@unisb.hr

Sažetak: Cilj ovog rada je analiza međugeneracijske (vertikalne) performativne multimedijske umjetnosti kao ujedinjene primarne, sekundarne i tercijarne edukacije. Ta modularna edukacija realizira se istraživačkom metodom globalnog i lokalnog pristupa filozofiji egzistencije, poznatoj kao glokalizacija. Multimedijalnim pristupom i učenjem na daljinu (e-learning) organiziraju se kroz grupnu orkestraciju veliki umjetnički performansi u izvannastavnim aktivnostima, na glavnom gradskom trgu, a za sve to svakako je potrebno otporno i sigurno digitalno okružje.

Ključne riječi: modularno obrazovanje, performativna multimedijska umjetnost, glokalizacija, kibernetička sigurnost

Modular, performative multimedia art

Abstract: The aim of this paper is the analysis of intergenerational (vertical) performative multimedia art as a unified primary, secondary and tertiary education. This modular education is realized through a research method of global and local approach to the philosophy of existence, known as glocalization. With multimedia access and distance learning (e-learning), large artistic performances are organized through group orchestration in extracurricular activities, in the main city square, and for all this, a resilient and secure digital environment is essential.

Keywords: modular education, performative multimedia art, glocalization, cybersecurity

Sigurnost bolesnika tijekom liječenja u Odjelu za neurologiju

prim. dr. sc. Lidija Šapina, dr. med. spec. neurolog[1], mr. sc. Krešimir Šapina, dipl. ing.[2]

[1] Opća bolnica Dr.Josip Benčević, Slavonski Brod, Hrvatska, lsapinasb@gmail.com

[2]Agroslavonija, Slavonski Brod, Hrvatska, jzksapina7@gmail.com

Sažetak: Sigurnosne mjere u zdravstvenim ustanovama, a posebno tijekom liječenja u odjelima za neurologiju važne su zbog povećanog rizika od različitih komplikacija i incidenata. Bolesnici u ovim odjelima često su poremećene svijesti, motorike, osjeta, koordinacije, kognitivno disfunkcionalni i doživljavaju epileptičke napade, što ih čini osjetljivijima na ozljede.

Ključne sigurnosne mjere su: 1. Prevencija padova: procjena rizika od pada pri prijemu (npr. Morse Fall Scale), održavanje prostora bez prepreka (kablovi, namještaj, seenzori pokreta na krevetima, pravilno podešeni bočni oslonci kreveta, protuklizne papuče. 2. Prevencija epileptičkih napada i ozljeda : redovita primjena antiepileptičke terapije, promatranje pacijenata s poznatim napadajima, osiguranje prostora oko pacijenta tijekom napada, brza medicinska intervencija kod epileptičnog napada /statusa. 3. Prevencija dekubitusa: Redovito okretanje nepokretnih pacijenata (svaka 2 sata), korištenje antidekubitalnih madraca i jastuka, njega kože i praćenje rizičnih točaka (sakrum, pete, itd.). 4. Osiguranje svijesti i orijentacije: pomoć kod dezorijentiranih pacijenata (npr. demencija, moždani udar), Vizualne i verbalne upute (sat, kalendar, informacije o danu), Prisustvo osoblja ili članova obitelji ako je moguće. 5. Zaštita od aspiracije: pravilno postavljanje pacijenta kod hranjenja (uspravan položaj), procjena sposobnosti gutanja (logoped, neurolog), prilagodba konzistencije hrane (npr. pasirana hrana). 6. Osiguranje lijekova i terapije: točna identifikacija pacijenta prije davanja lijekova, trostruka provjera (pacijent – lijek – doza), praćenje nuspojava neurološke terapije (npr. sedacija, promjene svijesti). 7. Psihološka sigurnost: empatična komunikacija, posebno kod pacijenata s afazijom ili kognitivnim poremećajima, uključivanje obitelji u skrb kada je moguće.

Ključne riječi: sigurnost, prevencija, medikacija, psihološka sigurnost

The safety of patients treated in the Neurology Department

Abstract: Safety measures in healthcare institutions, especially during treatment in neurology departments, are important due to the increased risk of various complications and incidents. Patients in these departments often have altered consciousness, motor skills, sensory perception, coordination, cognitive dysfunction, and experience epileptic seizures, which makes them more susceptible to injuries. Key safety measures include: 1. Fall prevention: assessing fall risk upon admission (e.g., Morse Fall Scale), maintaining clear spaces (cables, furniture, motion sensors on beds, properly adjusted side rails on beds, non-slip slippers). 2. Prevention of epileptic seizures and injuries: regular administration of antiepileptic therapy, monitoring patients with known seizures, ensuring space around the patient during a seizure, quick medical intervention in the event of an epileptic seizure/status. 3. Pressure ulcer prevention: regularly turning immobile patients (every 2 hours), using anti-decubitus mattresses and cushions, Skin care and monitoring of risk areas (sacrum, heels, etc.). 4. Ensuring awareness and orientation: assistance for disoriented patients (e.g. dementia, stroke), visual and verbal instructions (watch, calendar, information about the day), presence of staff or family members if possible. 5. Protection from aspiration: proper positioning of the patient during feeding (upright position), assessment of swallowing ability (speech therapist, neurologist), adjustment of food consistency (e.g. pureed food). 6. Ensuring medication and therapy: accurate patient identification before administering medication, triple-check (patient - medication - dose), monitoring side effects of neurological therapy (e.g. sedation, changes in consciousness). 7. Psychological safety: empathetic communication, especially with patients with aphasia or cognitive disorders, involving families in care when possible.

Keywords: safety, prevention, medication, psychological safety

Digitalne tehnologije u obrazovanju

izv. prof. dr. sc. Jasna Šego[1], dr. sc. Željka Rosandić, v. pred.[2]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, jsego@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, zrosandic@unisb.hr

Sažetak: Pandemija COVID-19 ubrzala je primjenu digitalnih tehnologija u obrazovanju, naglašavajući potrebu prilagodbe odgojno-obrazovnog sustava suvremenim tehnološkim alatima. Cilj je ovog rada analizirati utjecaj digitalnih tehnologija na obrazovni proces, s naglaskom na profesionalni razvoj nastavnika, obrazovna postignuća učenika i unaprjeđenje sustava. Rad nudi prijedloge za učinkovitu integraciju digitalnih alata, uzimajući u obzir tehničke, pedagoške i socijalne čimbenike. Korištene metode obuhvaćaju analizu literature, kvantitativne i kvalitativne studije slučaja o primjeni digitalnih alata u nastavi. Rezultati istraživanja pokazuju da digitalne tehnologije pozitivno utječu na profesionalni razvoj nastavnika unapređivanjem njihovih tehnoloških vještina i pristupa nastavi. Potiču razvoj vještina pismenosti, računalnog razmišljanja, kreativnosti, sposobnosti rješavanja problema i emocionalne kontrole. S obzirom na izazove tradicionalnog obrazovnog modela, digitalne tehnologije omogućuju individualan pristup učenju, povećavaju motivaciju za učenje i poučavanje te poboljšavaju interakciju nastavnika i učenika. Integracija digitalnih tehnologija u obrazovni sustav ne samo da unaprjeđuje pedagoški rad, nego i oblikuje moderne strategije za budući razvoj obrazovnog sustava. Rad potiče uporabu digitalne tehnologije u nastavi radi poboljšanja digitalne pismenosti nastavnika i učenika kao i uporabu novih znanja u svim fazama i raznolikim područjima odgojno-obrazovnog rada.

Ključne riječi: digitalne tehnologije, integracija tehnologije, motivacija, obrazovni sustav, pismenost, profesionalni razvoj

Digital technologies in education

Abstract: The COVID-19 pandemic has accelerated the application of digital technologies in education, emphasizing the need to adapt the educational system to modern technological tools. The goal of this paper is to analyse the impact of digital technologies on the educational system, with a focus on the professional development of teachers, students' educational achievements, and system improvement. The paper offers suggestions for the effective integration of digital tools, considering technical, pedagogical, and social factors. The methods used include literature analysis, as well as quantitative and qualitative case studies on the application of digital tools in teaching. The research results show that digital technologies positively affect the professional development of teachers by enhancing their technological skills and teaching approach. They promote the development of literacy skills, computational thinking, creativity, problem-solving abilities, and emotional control. Given the challenges of the traditional educational model, digital technologies enable individualized learning, increase motivation for learning and teaching, and improve teacher-student interaction. The integration of digital technologies into the educational system not only enhances pedagogical work but also shapes modern strategies for the future development of the educational system. The study encourages the use of digital technology in teaching to improve the digital literacy of teachers and students, as well as the application of new knowledge in all phases and diverse areas of educational work.

Keywords: digital technologies, technology integration, motivation, educational system, literacy, professional development

Analiza naplate plasmana poslovnih subjekata kod banaka u kontekstu kibernetičke sigurnosti

doc. dr. sc. Maja Vretenar Cobović[1], Marina Brčelić Kovačević, studentica[2]

[1] Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, mvcobovic@unisb.hr

[2]Sveučilište u Slavonskom Brodu, Slavonski Brod, Hrvatska, mbrcelic@unisb.hr

Sažetak: U suvremenom bankarskom poslovanju, učinkovita naplata plasmana poslovnim subjektima neraskidivo je povezana s osiguranjem kibernetičke sigurnosti. Složen proces naplate obuhvaća kontinuirano praćenje dospjelih obveza za različite vrste plasmana (dugoročni i kratkoročni krediti, revolving krediti, garancije i dr.). Kreditni plasmani i garancije, kao značajan dio bankarskog portfelja, predstavljaju kompleksan i obiman segment naplate, zahtijevajući precizno praćenje dinamike plaćanja i promptnu reakciju na eventualna kašnjenja. Komunikacija s poslovnim subjektima tijekom procesa naplate izložena je sve većem riziku kibernetičkih napada, čime kibernetička sigurnost postaje nezaobilazan element. Ovaj rad stoga ima za cilj detaljno opisati proces naplate plasmana poslovnih subjekata te istražiti i analizirati njegovu povezanost s kibernetičkom sigurnošću. Autori u radu koriste niz znanstvenih metoda istraživanja (metode analize, komparacije, indukcije, dedukcije, deskripcije i klasifikacije itd.) kao i pojedine statističko-matematičke metode. Metodologija istraživanja temeljena je na metodi ankete putem instrumenta online anketnog upitnika. Dobiveni rezultati istraživanja pokazuju da određena razina kibernetičke sigurnosti značajno doprinosi uspješnosti naplate plasmana unutar bankarskog sustava.

Ključne riječi: banke, kibernetička sigurnost, kreditni plasmani, poslovni subjekti

Analysis of collection of placement from business entities with banks in the context of cybernetic security

Abstract: In modern banking business, effective collection of placements from business entities is inextricably linked to ensuring cybersecurity. The complex collection process includes continuous monitoring of overdue obligations for various types of placements (long-term and short-term loans, revolving loans, guarantees, etc.). Credit placements and guarantees, as a significant part of the banking portfolio, represent a complex and large-scale collection segment, requiring precise monitoring of payment dynamics and prompt reaction to possible delays. Communication with business entities during the collection process is exposed to an increasing risk of cyberattacks, which makes cyber security an indispensable element. This paper therefore aims to describe in detail the process of collecting placements from business entities and to investigate and analyze its connection with cybersecurity. In the paper, the authors use a number of scientific research methods (methods of analysis, comparison, induction, deduction, description, and classification, etc.), as well as certain statistical and mathematical methods. The research methodology is based on the survey method using an online questionnaire. The research results show that a certain level of cybersecurity significantly contributes to the effectiveness of loan collection within the banking system.

Keywords: banks, cybersecurity, credit placements, business entities

Percepcije učenika o učenju temeljenom na digitalnim igrama

Marijana Zarožinski, dipl. ing. mat., asist.[1], izv. prof. dr. sc. Ljerka Jukić Matić[2], Maja Čuletić Čondrić, prof. mat. i fiz., pred.[3]

[1] Industrijsko-obrtnička škola Slavonski Brod, Slavonski Brod, Hrvatska, marijanazarozinski@gmail.com

[2]Fakultet primijenjene matematike i informatike, Osijek, Hrvatska, ljukic@mathos.hr

[3]Sveučilište u Slavonskm Brodu, Slavonski Brod, Hrvatska, mccondric@unisb.hr

Sažetak: U kontekstu sveprisutne tehnologije, rad istražuje potencijal digitalnih igara u nastavi matematike (DGBL) s fokusom na učeničke perspektive u Hrvatskoj. Pregled literature ukazuje na pozitivne učinke DGBL-a na motivaciju i angažman, no domaća istraživanja o stavovima učenika prema DGBL-u u matematici su nedostatna. Svrha rada je istražiti stavove i motivaciju učenika u Hrvatskoj prema korištenju DGBL-a u nastavi matematike. Cilj je izraditi i pilotirati anketni upitnik za mjerenje tih stavova i motivacije. Metoda uključuje pregled literature i izradu anketnog upitnika temeljenog na postojećim instrumentima, s planiranim pilot projektom u Industrijsko-obrtničkoj školi. Očekuje se da će upitnik biti pouzdan i da će učenici imati pozitivan stav prema učenju matematike pomoću digitalnih igara. Ovaj rad doprinosi razumijevanju učeničkih perspektiva o DGBL-u u hrvatskom obrazovnom kontekstu te donosi osvrt na sigurnosne aspekte, otvarajući put za daljnja istraživanja i potencijalnu implementaciju.

Ključne riječi: učenje temeljeno na digitalnim igrama (DGBL), igre, matematika, stavovi učenika, motivacija, učenici strukovnih škola

Student perceptions of Digital Game Based Learning

Abstract: In the context of ubiquitous technology, the paper explores the potential of digital games in mathematics education (DGBL) with a focus on students' perspectives in Croatia. The literature review indicates positive effects of DGBL on motivation and engagement, but domestic research on students' attitudes towards DGBL in mathematics is insufficient. The purpose of the paper is to investigate students' attitudes and motivation in Croatia towards the use of DGBL in mathematics education. The aim is to develop and pilot a survey questionnaire to measure these attitudes and motivation. The method includes a literature review and the development of a survey questionnaire based on existing instruments, with a planned pilot project in an Industrial and Craft School. It is expected that the questionnaire will be reliable and that students will have a positive attitude towards learning mathematics using digital games. This paper contributes to understanding students' perspectives on DGBL in the Croatian educational context and provides a review of safety aspects, paving the way for further research and potential implementation.

Keywords: Digital Game Based Learning (DGBL), games, mathematics, student attitudes, motivation, vocational students

ISBN: 978-953-8426-05-6