Pučko otvoreno učilište Čakovec

Ulica kralja Tomislava 52, 40 000 Čakovec

Program obrazovanja
za stjecanje mikrokvalifikacije
sigurnost informacijskih sustava

Čakovec, ožujak 2022.

1. OPĆI DIO

<table>
<tr><th colspan="4">OPĆE INFORMACIJE O PROGRAMU OBRAZOVANJA
ZA STJECANJE MIKROKVALIFIKACIJE</th></tr>
<tr><td>Sektor</td><td colspan="3">Elektrotehnika i računarstvo</td></tr>
<tr><td>Naziv programa</td><td colspan="3">Program obrazovanja za stjecanje mikrokvalifikacije sigurnost informacijskih sustava</td></tr>
<tr><td>Vrsta programa</td><td colspan="3">Usavršavanje</td></tr>
<tr><td rowspan="2">Predlagatelj</td><td>Naziv ustanove</td><td colspan="2">Pučko otvoreno učilište Čakovec</td></tr>
<tr><td>Adresa</td><td colspan="2">Ulica kralja Tomislava 52, 40 000 Čakovec</td></tr>
<tr><td>Razina kvalifikacije/skupa/ova ishoda učenja prema HKO-u</td><td colspan="3">SIU 1: ZAŠTITA RAČUNALNE MREŽE (razina 4)
SIU 2: KRIPTOGRAFIJA (razina 4)</td></tr>
<tr><td>Obujam u bodovima (CSVET)</td><td colspan="3">3 CSVET
SIU 1: ZAŠTITA RAČUNALNE MREŽE (2 CSVET)
SIU 2: KRIPTOGRAFIJA (1 CSVET)</td></tr>
<tr><th colspan="4">Dokumenti na temelju kojih je izrađen program obrazovanja za stjecanje kvalifikacija/skupova ishoda učenja (mikrokvalifikacija)</th></tr>
<tr><td>Popis standarda zanimanja/skupova kompetencija i datum/i njegove/njihove valjanosti u Registru HKO-a</td><td colspan="2">Popis standarda kvalifikacija/skupova ishoda učenja i datum/i njegove/njihove valjanosti u Registaru HKO-a</td><td>Sektorski kurikulum</td></tr>
<tr><td>SZ Tehničar za računarstvo

SKOMP 1: Primjena računalne sigurnosti https://hko.srce.hr/registar/skup-kompetencija/detalji/163

SKOMP2: Dijagnosticiranje programskih i/ili sistemskih problema https://hko.srce.hr/registar/skup-kompetencija/detalji/158

31.12.2022.</td><td colspan="2">SIU Zaštita računalne mreže

SIU Kriptografija

15.12.2024.</td><td></td></tr>
<tr><td>Uvjeti za upis u program</td><td colspan="3">Cjelovita kvalifikacija minimalno na razini 4.1</td></tr>
<tr><td>Uvjeti stjecanja programa (završetka programa)</td><td colspan="3">• Stečena 3 CSVET boda
• Uspješna završna provjera stečenih znanja usmenim i/ili pisanim provjerama te vještina polaznika kroz projektne i problemske zadatke, a temeljem unaprijed određenih kriterija vrednovanja postignuća.
• Na završnoj provjeri vodi se zapisnik i provodi ju tročlano povjerenstvo.</td></tr>
</table>

	• Svakom polazniku nakon uspješno završene završne provjere izdaje se Uvjerenje o usavršavanju za stjecanje mikrokvalifikacije sigurnost informacijskih sustava
Trajanje i načini izvođenja nastave	Program obrazovanja za stjecanje mikrokvalifikacije sigurnost informacijskih sustava provodi se redovitom nastavom u trajanju od 75 sati, uz mogućnost izvođenja teorijskog dijela programa na daljinu u realnom vremenu. Ishodi učenja ostvaruju se dijelom vođenim procesom učenja i poučavanja u trajanju od 20 sati, dijelom učenjem temeljenom na radu u trajanju od 40 sati, a dijelom samostalnim aktivnostima polaznika u trajanju od 15 sati. Učenje temeljeno na radu obuhvaća situacijsko učenje i izvršenje konkretnih radnih zadaća u stavarnim i/ili simuliranim uvjetima.
Horizontalna prohodnost	Prema kvalifikaciji tehničar za računalstvo
Vertikalna prohodnost	
Materijalni uvjeti i okruženje za učenje koji su potrebni za izvedbu programa	Specijalizirana učionica opremljena s radnim stolovima s umreženim računalima s instaliranom potrebnom programskom potporom i pristupom internetu i/ili lokalnoj mreži, centralno upravljačko mjesto nastavnika s umreženim računalom za upravljanje svih priključaka na radnim mjestima polaznika, mjernim instrumentima, alatom i opremom, komponentama i/ili sklopovima, vatrozid (hardverski ili softverski), poslužitelj s poslužiteljskim operacijskim sustavom, neprekidno napajanje, sustav za e-učenje s dostupnim elektroničkim materijalima i pristupom različitim online aktivnostima.
Kompetencije koje se programom stječu	
1. interpretirati etičke osnove računalne sigurnosti 2. primijeniti postupke i procedure za zaštitu osobnih podataka korisnika 3. održavati zapise o sigurnosti i razinama pristupa imovini organizacije 4. dijagnosticirati jednostavne probleme u radu računalnih sustava i mreža	
Preporučeni načini praćenja kvalitete i uspješnosti izvedbe programa	U procesu praćenja kvalitete i uspješnosti izvedbe programa obrazovanja primjenjuju se sljedeće aktivnosti: • provodi se istraživanje i anonimno anketiranje polaznika o izvođenju nastave, literaturi i resursima za učenje, strategijama podrške polaznicima, izvođenju i unapređenju procesa učenja i poučavanja, radnom opterećenju polaznika (CSVET), provjerama znanja te komunikaciji s nastavnicima • provodi se istraživanje i anketiranje nastavnika o istim pitanjima navedenim u prethodnoj stavci • provodi se analiza uspjeha, transparentnosti i objektivnosti provjera i ostvarenosti ishoda učenja • provodi se analiza materijalnih i kadrovskih uvjeta potrebnih za izvođenje procesa učenja i poučavanja. Dobivenim rezultatima anketa dobiva se pregled uspješnosti izvedbe programa, kao i procjena kvalitete nastavničkog rada. Postupci vrednovanja usmjereni su na praćenje i provjeru postignuća prema ishodima učenja. Ono se provodi usmenim i pisanim provjerama znanja te provjerama stečenih vještina polaznika projektnim i problemskim zadatcima te radnim situacijama, a temeljem unaprijed određenih kriterija vrednovanja postignuća.
Datum revizije programa	

2. MODULI I SKUPOVI ISHODA UČENJA

Redni broj	NAZIV MODULA	POPIS SKUPOVA ISHODA UČENJA	Razina	Obujam CSVET	Broj sati			
					VPUP	UTR	SAP	UKUPNO
1.	Sigurnost informacijskih sustava	Zaštita računalne mreže	4	2	10	30	10	50
		Kriptografija	4	1	10	10	5	25
Ukupno:				**3**	**20**	**40**	**15**	**75**

VPUP – vođeni proces učenja i poučavanja
UTR – učenje temeljeno na radu
SAP– samostalne aktivnostipolaznika

3. RAZRADA MODULA I SKUPOVA ISHODA UČENJA

NAZIV MODULA	**SIGURNOST INFORMACIJSKIH SUSTAVA**		
Šifra modula			
Kvalifikacije nastavnika koji sudjeluju u realizaciji modula	• najmanje razina 6 HKO-a – 180 ECTS bodova (preddiplomski sveučilišni studij, preddiplomski stručni studij) odgovarajućeg profila.		
Obujam modula (CSVET)	**5 CSVET**		
Načini stjecanja ishoda učenja (od – do, postotak)	**Vođeni proces učenja i poučavanja**	**Oblici učenja temeljenog na radu**	**Samostalne aktivnosti polaznika**
	20 (27%)	40 (53%)	15 (20%)
Status modula (obvezni/izborni)	obvezni		
Cilj (opis) modula	Cilj modula je polaznicima omogućiti stjecanje kompetencija analiziranja i konfiguriranja zaštite računalne mreže postavljanjem sigurnosnih politika informacijskog sustava, korištenje alata za praćenje mrežnog prometa i kriptografije.		
Ključni pojmovi	*sigurnosne politike, zaštita mrežnih uređaja, sigurnosni rizici, kriptografija*		
Oblici učenja temeljenog na radu	Učenje temeljeno na radu ostvaruje se realiziranjem radnih zadataka koji se mogu simulirati u školskim specijaliziranim učionicama/praktikumima ili u Regionalnim centrima kompetentnosti. Poželjno je koristiti projektnu i istraživačku nastavu te situacijsko učenje i poučavanje odnosno zadaci za učenje i vježbanje trebaju odgovarati stvarnim radnim situacijama nekog radnog mjesta. Isto tako, gdje god je to moguće, ishode učenja kojima polaznik stječe praktične vještine treba ostvariti u realnim uvjetima kod poslodavca (gospodarski subjekt s kojim ustanova ostvaruje poslovnu suradnju). Zadaci/projekti mogu biti na temu analize trenutne razine sigurnosti u mreži, izračunavanje sigurnosnog rizika, poboljšanje sigurnosti mreže na veću razinu, podešavanje sigurnosti mrežnih uređaja za potrebe poslovnog subjekta i sl.		

Literatura i specifična nastavna sredstva potrebna za realizaciju modula	1. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Cengage Learning, 2017. 2. Calder, A: IT governance : a manager's guide to data security and ISO 27001/ISO 27002 3. ISO/IEC 27002:2013: Information technology, Security techniques: Code of practice for information security controls 4. ISO/IEC 27001:2013: Information technology, Security techniques: Information Security Management Systems, Requirements

Skup ishoda učenja iz SK-a[1]:	**ZAŠTITA RAČUNALNE MREŽE**
Ishodi učenja	
1. Primijeniti osnovna načela u izgradnji sigurnosne politike informacijskog sustava poslovnog subjekta 2. Postaviti zaštitu na mrežnim uređajima prema specifikaciji 3. Konfigurirati zaštitu mreže u lokalnoj mreži poslovnog subjekta 4. Otkloniti sigurnosne rizike na mreži poslovnog subjekta 5. Koristiti alate za praćenje mrežnog prometa u mreži poslovnog subjekta	
Dominantan nastavni sustav i opis načina ostvarivanja SIU	
Dominantan nastavni sustav je učenje temeljeno na radu kroz projektnu nastavu i rad u timovima na rješavanju poslovnog zadatka primjenom osnovnih načela sigurnosti, postavljanjem zaštite uređaja te korištenjem alata za praćenje mrežnog prometa s obzirom na potrebe korisnika u što realnijoj poslovnoj situaciji. Nastavnik u ulozi mentora organizira i usmjerava aktivnosti polaznika te im pomaže u pretvaranju poslovnog scenarija u konkretne akcije. Polaznici preporučuju zaštite na mrežnim uređajima pronalazeći specifikacije raznih vrsta zaštita i uspoređuju ih s potrebama korisnika. Pri radu nastavnik usmjerava polaznike prema detekciji i otklanjanju problema.	
Nastavne cjeline/teme	– Informacijski sustav – Načela sigurnosnih politika – Sigurnosni rizici – Fizička sigurnost – Alati za praćenje mrežnog prometa
Načini i primjer vrjednovanja skupa ishoda učenja	

Želim sigurnu mrežu

Tvrtka koja se bavi razvojem softvera ima velik broj računala u svojoj računalnoj mreži. Potrebna im je analiza trenutne razine sigurnosti u mreži, sigurnosni rizik te prijedlog unaprjeđenja sigurnosti mreže na najveću moguću razinu.

Uputa: Polaznike podijeliti u timove od tri do četiri člana sa zadacima:

- Pomoću osnovnih načela sigurnosti i korištenjem alata za praćenje mrežnog prometa procijeniti razinu sigurnosti u mreži i preporučiti poboljšanje sigurnosti
- Postaviti zaštitu na mrežnim uređajima u mreži poslovnog subjekta i otkloniti sigurnosne rizike.

Vrednovanje naučenog: vrednuje se odabrano tehničko rješenje iz zadatka, javna prezentaciju te doprinos rješavanju zadatka

Element/kriterij vrednovanja	**5 bodova**	**4 boda**	**3 boda**	**2 boda**

[1]Popunjava se onoliko puta koliko je skupova ishoda učenja u modulu.

Procjena sigurnosti I preporuka poboljšanja razine sigurnosti	Polaznik samostalno procjenjuje trenutnu sigurnost računalne mreže samostalno te daje preporuke za poboljšanje sigurnosti	Polaznik samostalno procjenjuje trenutnu sigurnost mreže te daje preporuke za poboljšanje sigurnosti računalne mreže uz manje pogreške	Polaznik uz povremenu pomoć procjenjuje trenutnu sigurnost računalne mreže	Polaznik samo uz pomoć procjenjuje trenutnu sigurnost računalne mreže
Postavljanje zaštite na mrežnim uređajima u mreži poslovnog subjekta i otklanjanje sigurnosnih rizika	Polaznik samostalno konfigurira zaštitu na mrežnim uređajima I ispravnim postavljanjem otklanja sigurnosne rizike te daje prijedloge za poboljšanje	Polaznik samostalno konfigurira zaštitu na mrežnim uređajima I ispravnim postavljanjem otklanja sigurnosne rizike uz manje greške	Polaznik uz povremenu pomoć konfigurira zaštitu na mrežnim uređajima I ispravnim postavljanjem otklanja sigurnosne rizike	Polaznik samo uz pomoć konfigurira zaštitu na mrežnim uređajima I ispravnim postavljanjem otklanja sigurnosne rizike
Korištenje alata za praćenje mrežnog prometa	Polaznik samostalno koristi alat za praćenje mrežnog prometa	Polaznik koristi alat za praćenje mrežnog prometa uz manje greške	Polaznik koristi alat za praćenje mrežnog prometa uz povremenu pomoć	Polaznik koristi alat za praćenje mrežnog prometa samo uz pomoć nastavnika

Prema ostvarenim bodovima izrađuje se ljestvica i prijedlog ocjena.

Vrednovanje za učenje: tablica za praćenje aktivnosti učenika za vrijeme rada:

Elementi procjene	Potpuno	Djelomično	Potrebno doraditi
Polaznik se pripremio za projektnu nastavu prema uputama nastavnika			
Polaznik surađuje s ostalim članovima tima			
Polaznik izvršava svoj dio zadatka			
Polaznik sudjeluje u prezentaciji dobivenih rezultata			

Prilagodba iskustava učenja za polaznike/osobe s invaliditetom

(Izraditi način i primjer vrjednovanja skupa ishoda učenja za polaznike/osobe s invaliditetom ako je primjenjivo)

Skup ishoda učenja iz SK-a:	**KRIPTOGRAFIJA**

Ishodi učenja

1. Analizirati nekriptirane poruke mrežnih uređaja
2. Konfigurirati kriptografiju na mrežnim uređajima
3. Na osnovi usporedbe rezultata analize nekriptiranih i kriptiranih poruka zaključiti o razini sigurnosti računalne mreže

Dominantan nastavni sustav i opis načina ostvarivanja SIU

Dominantan nastavni sustav je učenje temeljeno na radu kroz projektnu nastavu i rad u timovima na rješavanju poslovnog zadatka primjenom raznih alata za analiziranje nekriptiranih i kriptiranih poruka na mrežnim uređajima te konfiguriranjem kriptografske zaštite zaključuje o razini sigurnosti računalne mreže s obzirom na potrebe korisnika u što realnijoj poslovnoj situaciji. Nastavnik u ulozi mentora organizira i usmjerava aktivnosti polaznika te im pomaže u pretvaranju poslovnog scenarija u konkretne akcije. Polaznici preporučuju kriptografsku zaštitu na mrežnim uređajima pronalazeći specifikacije raznih vrsta kriptografskih zaštita i uspoređuju ih s potrebama korisnika.

Nastavne cjeline/teme	– Kriptografija – Enkripcija – Dekripcija – Kriptografski algoritmi

Načini i primjer vrjednovanja skupa ishoda učenja

Testiraj i postavi enkripciju računalne mreže

Podešavanje sigurnosti mrežnih uređaja za potrebe poslovnog subjekta na osnovu testiranja razine sigurnosti mreže te analiziranjem kriptiranih i nekriptiranih poruka.

Uputa: Polaznike podijeliti u timove od tri do četiri člana gdje svaki tim podešava sigurnost u svojoj bežičnoj računalnoj mreži.

Vrednovanje naučenog: nastavnik vrednuje odabrano tehničko rješenje iz zadatka, javnu prezentaciju te doprinos rješavanju zadatka po elementima:

- Ispitivanje razine sigurnosti bežične računalne mreže
- Konfiguracija enkripijske zaštite na mrežnim uređajima
- Prezentiranje rezultata analize razine sigurnosti računalne mreže na osnovu praćenja kriptiranih I nekriptiranih poruka u mreži

Prilagodba iskustava učenja za polaznike/osobe s invaliditetom

(Izraditi način i primjer vrjednovanja skupa ishoda učenja za polaznike/osobe s invaliditetom ako je primjenjivo)

***Napomena:**

Riječi i pojmovni sklopovi koji imaju rodno značenje korišteni u ovom dokumentu (uključujući nazive kvalifikacija, zvanja i zanimanja) odnose se jednako na oba roda (muški i ženski) i na oba broja (jedninu i množinu), bez obzira na to jesu li korišteni u muškom ili ženskom rodu, odnosno u jednini ili množini.

Broj i datum mišljenja na program (popunjava Agencija):

KLASA:	
URBROJ:	
Datum izdavanja mišljenja na program:	