**Naziv i adresa ustanove**

**Program obrazovanja**

**za stjecanje mikrokvalifikacije**

**sigurnost informacijskih sustava**

**Mjesto, datum**

1. **OPĆI DIO**

|  |  |  |  |
| --- | --- | --- | --- |
| **OPĆE INFORMACIJE O PROGRAMU OBRAZOVANJA**  **ZA STJECANJE MIKROKVALIFIKACIJE** | | | |
| **Sektor** | Elektrotehnika i računarstvo | | |
| **Naziv programa** | Program obrazovanja za stjecanje mikrokvalifikacije sigurnost informacijskih sustava | | |
| **Vrsta programa** | Osposobljavanje | | |
| **Predlagatelj** | **Naziv ustanove** |  | |
| **Adresa** |  | |
| **Razina kvalifikacije/skupa/ova ishoda učenja prema HKO-u** | SIU 1: Sigurnost i zaštita mrežnih sustava (razina 4)  SIU 2: Kriptografija(razina 4) | | |
| **Obujam u bodovima (CSVET)** | **3 CSVET**  SIU 1: Sigurnost i zaštita mrežnih sustava (2 CSVET)  SIU 2: Kriptografija(1 CSVET) | | |
| **Dokumenti na temelju kojih je izrađen program obrazovanja za stjecanje kvalifikacija/skupova ishoda učenja (mikrokvalifikacija)** | | | |
| **Popis standarda zanimanja / skupova kompetencija** | **Popis standarda kvalifikacija / skupova ishoda učenja** | | **Sektorski kurikulum** |
| **SK Tehničar za informacijske tehnologije / Tehničarka za informacijske tehnologije**  <https://hko.srce.hr/registar/standard-zanimanja/detalji/505>  **SKOMP 1:** Zaštićivanje IT sustava  <https://hko.srce.hr/registar/skup-kompetencija/detalji/4145> | **SK Tehničar za informacijske tehnologije / Tehničarka za informacijske tehnologije**  <https://hko.srce.hr/registar/standard-kvalifikacije/detalji/443>  **SIU 1: Sigurnost i zaštita mrežnih sustava**  <https://hko.srce.hr/registar/skup-ishoda-ucenja/detalji/8131>  **SIU 2: Kriptografija**  <https://hko.srce.hr/registar/skup-ishoda-ucenja/detalji/1069> | |  |
| **Uvjeti za upis u program** | - posjedovanje cjelovite kvalifikacije minimalno na razini 4.1 HKO-a | | |
| **Uvjeti stjecanja programa (završetka programa)** | * 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.   Svakom polazniku nakon uspješno završene završne provjere izdaje se Uvjerenje o osposobljavanju 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** |  | | |
| **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.  <https://hko.srce.hr/registar/skup-ishoda-ucenja/detalji/8131>  <https://hko.srce.hr/registar/skup-ishoda-ucenja/detalji/1069>  Sukladno članku 22. stavku 1. Zakona o obrazovanju odraslih (Narodne novine br. 144/21), prema kojem je ustanova obvezna voditi brigu o pravima polaznika i pristupnika, postupati etično i na dobrobit polaznika i pristupnika, ustanova je dužna upoznati polaznika sa zdravstvenim zahtjevima potrebnim za stjecanje kvalifikacije. Polaznika se upoznaje sa zdravstvenim zahtjevima potrebnima u procesu stjecanja ishoda učenja, zdravstvenim zaprekama za zanimanje, opisom radnih zadaća, kao i uvjetima rada u zanimanju za koje polaznik upisuje program.  Nakon što je polaznik upoznat s navedenim, a u slučaju da zbog specifičnih zdravstvenih zahtjeva ili mogućih zdravstvenih ograničenja dođe do teškoća tijekom obrazovanja, zapošljavanja ili rada, uključujući nemogućnost ili ograničenu mogućnost obrazovanja, zapošljavanja ili obavljanja radnih zadataka, odgovornost preuzima sam polaznik.  Neovisno o zdravstvenim specifičnostima polaznika, ustanova je obvezna osigurati jednak pristup obrazovanju svim polaznicima, uz stalno poštivanje prava na zdravlje i sigurnost, osobito tijekom učenja temeljenog na radu. Ustanova i poslodavac kod kojega se odvija učenje temeljeno na radu odgovorni su za osiguravanje uvjeta rada koji ne ugrožavaju zdravlje polaznika.  Preporučuje se da polaznik i odgovorna osoba ustanove potpišu izjavu kojom potvrđuju upoznatost s prethodno navedenim informacijama o ukupnim zahtjevima zanimanja iz programa koji polaznik upisuje. Sadržaj izjave određuje sama ustanova, pri čemu forma nije propisana.  Podloga za primjenu jedinstvenog popisa zdravstvenih zahtjeva potrebnih za upis u pojedinom zanimanju je dokument objavljen na mrežnim stranicama Ministarstva znanosti, obrazovanja i mladih *[Jedinstveni popis zdravstvenih zahtjeva potrebnih za upis u strukovne kurikule u I. razred srednje škole](https://mzom.gov.hr/UserDocsImages/dokumenti/Dokumenti-ZakonskiPodzakonski-Akti/Jedinstveni-popis-zdravstvenih-zahtjeva-potrebnih-za-upis-u-strukovne-kurikule-u-I-razred-srednje-skole-2025.pdf" \t "_blank)*, pri čemu posebno ukazujemo na popis zdravstvenih zapreka koje predstavljaju apsolutnu zapreku za pojedino zanimanje.  Ujedno napominjemo, ako je za stjecanje kompetencija u okviru pojedinog programa osposobljavanja, usavršavanja ili specijalističkog usavršavanja, zbog specifičnosti radnih zadaća i radnog okruženja, potreban dokaz o procjeni zdravstvenih sposobnosti polaznika te je isto navedeno kao obvezujuće u Jedinstvenom popisu zdravstvenih zahtjeva potrebnih za upis u strukovne kurikule u I. razred srednje škole, polaznik je dužan dostaviti dokaz o zdravstvenoj sposobnosti. | | |
| **Kompetencije koje se programom stječu** | | | |
| 1. Osmisliti unaprjeđenje sigurnosti jednostavnog IT sustava 2. Primijeniti mjere osiguravanja IT sustava 3. Upravljati sigurnošću jednostavnog IT sustava 4. Ukloniti sigurnosne prijetnje IT sustava | | | |
| **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** |  | | |

1. **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 | Sigurnost i zaštita mrežnih sustava | 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*

1. **RAZRADA MODULA I SKUPOVA ISHODA UČENJA**

|  |  |  |  |
| --- | --- | --- | --- |
| **NAZIV MODULA** | **SIGURNOST INFORMACIJSKIH SUSTAVA** | | |
| **Šifra modula** |  | | |
| **Kvalifikacije nastavnika koji sudjeluju u realizaciji modula** | <https://hko.srce.hr/registar/skup-ishoda-ucenja/detalji/8131>  <https://hko.srce.hr/registar/skup-ishoda-ucenja/detalji/1069> | | |
| **Obujam modula (CSVET)** | **3 CSVET** | | |
| **Načini stjecanja ishoda učenja (od – do, postotak)** | **Vođeni proces učenja i poučavanja** | **Oblici učenja temeljenog na radu** | **Samostalne aktivnosti polaznika** |
| 20 sati (27%) | 40 sati (53%) | 15 sati (20%) |
| **Status modula**  **(obvezni/izborni)** | obvezni | | |
| **Cilj (opis) modula** | Cilj modula je polaznicima omogućiti stjecanje znanja i vještina za analiziranje i konfiguriranje 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** | * Materijali za korisnike izrađeni u ustanovi * Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Cengage Learning, 2017. * Calder, A: IT governance : a manager’s guide to data security and ISO 27001/ISO 27002 * ISO/IEC 27002:2013: Information technology, Security techniques: Code of practice for information security controls * ISO/IEC 27001:2013: Information technology, Security techniques: Information Security Management Systems, Requirements | | |

|  |  |  |
| --- | --- | --- |
| **Skup ishoda učenja iz SK-a, obujam[[1]](#footnote-1):** | | **Sigurnost i zaštita mrežnih sustava, 2 CSVET** |
| **Ishodi učenja** | | |
| 1. Identificirati potencijalne sigurnosne prijetnje i ranjivosti u mrežnim sustavima | | |
| 1. Analizirati rizike i potencijalne posljedice sigurnosnih prijetnji na mrežne sustave | | |
| 1. Implementirati sigurnosne mehanizme i postavke u mrežne sustave | | |
| 1. Provoditi testiranje sigurnosti mrežnih sustava | | |
| 1. Spriječiti sigurnosne prijetnje u mrežnim sustavima | | |
| **Dominantan nastavni sustav i opis načina ostvarivanja SIU** | | |
| Dominantan nastavni sustav je učenje temeljeno na radu.  Polaznici pomoću stvarnih radnih situacija stječu znanja o potencijalnim opasnostima ili šteti koja može proizaći iz sigurnosne prijetnje na softverske sustave, alatima, tehnici i postavkama koje se implementiraju u softverske sustave radi zaštite od sigurnosnih prijetnji i usklađenosti s industrijskim normama i regulativama. | | |
| **Nastavne cjeline/teme** | Informacijski sustav  Načela sigurnosnih politika  Sigurnosni rizici  Fizička sigurnost  Alati za praćenje mrežnog prometa | |
| **Načini i primjer vrjednovanja skupa ishoda učenja** | | |
| Instalirati sigurnosni softver na korisničko računalo. Potrebno je osigurati da računalo bude zaštićeno od potencijalnih prijetnji i ranjivosti.  Koraci zadatka:   * Provjeriti je li već instaliran sigurnosni softver na računalu. Polaznik to može provjeriti otvaranjem odgovarajućeg softverskog sustava za sigurnost i provjerom postavki ili statusa sigurnosnog softvera. Ako nije instaliran sigurnosni softver, polaznik treba pronaći odgovarajući besplatni sigurnosni softver koji je kompatibilan s trenutačnim operacijskim sustavom računala. Može istražiti razne opcije putem interneta, pregledavajući *web*-stranice ili koristeći preporučene izvore. Nakon pronalaska odgovarajućeg sigurnosnog softvera, polaznik treba preuzeti instalacijski paket s *web*-stranice ili drugog izvora. Treba biti oprezan i preuzeti softver s pouzdanih izvora kako bi se izbjeglo preuzimanje zlonamjernog softvera. * Pokrenuti instalacijski program sigurnosnog softvera i pratiti upute za instalaciju. Uobičajeni postupak uključuje prihvaćanje licencnog ugovora, odabir željenih postavki i odredišnog mjesta za instalaciju softvera. * Nakon uspješne instalacije, polaznik treba provjeriti ima li dostupnih ažuriranja za sigurnosni softver. Većina softverskih sustava ima automatsku provjeru ažuriranja, ali polaznik bi trebao provjeriti jesu li sva ažuriranja instalirana i je li sigurnosni softver ažuriran na najnoviju verziju. * Nakon ažuriranja polaznik treba konfigurirati sigurnosni softver prema specifičnim potrebama računala: postavljanje različitih sigurnosnih postavki, odabir vrste skeniranja, postavljanje rasporeda ažuriranja ili prilagođavanje drugih značajki sigurnosnog softvera. * Kad je sigurnosni softver konfiguriran, polaznik treba provesti testiranje kako bi se osiguralo da softver ispravno funkcionira: izvođenje skeniranja računala, provjera detekcije prijetnji ili simuliranje napada kako bi se provjerila reakcija sigurnosnog softvera. * Nakon provedenog testiranja, polaznik treba analizirati prikupljene podatke kako bi identificirao eventualne prijetnje ili ranjivosti softverskog sustava: pregled izvješća o skeniranju, provjera logova sigurnosnog softvera ili analiza rezultata testiranja. | | |
| **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, obujam:** | | **Kriptografija, 1 CSVET** |
| **Ishodi učenja** | | |
| 1. Analizirati nekriptirane poruke mrežnih uređaja u mreži poslovnog subjekta | | |
| 1. Konfigurirati kriptografiju i VPN na mrežnim uređajima u mreži poslovnog subjekta | | |
| 1. Na osnovi usporedbe rezultata analize nekriptiranih i kriptiranih poruka zaključiti o razini sigurnosti računalne mreže 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 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** | | |
| Karlo je djelatnik u tvrtki koja se bavi zaštitom računalnih mreža te za klijentsku ustanovu priprema prezentaciju o kriptografiji. Karlo će:  a) Pomoću softvera za analizu mrežnih podataka uhvatiti podatke koji prolaze kroz aktivno mrežno sučelje i analizirati nekriptirane poruke.  b) Podesiti parametre mrežnih uređaja za izvođenje osnovnih mrežnih servisa koristeći kriptografjiu i VPN. Pomoću softvera za analizu mrežnih podataka uhvatiti podatke koji prolaze kroz aktivno mrežno sučelje i analizirati kriptirane poruke.  c) Usporediti rezultate analize nekriptiranih i kriptiranih poruka te procijeniti razinu sigurnosti mreže poslovnog subjekta. | | |
| **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: |  |

1. Popunjava se onoliko puta koliko je skupova ishoda učenja u modulu*.* [↑](#footnote-ref-1)