



UNIVERZITET U SARAJEVU

**Centar za interdisciplinarne studije - „prof. dr. Zdravko Grebo“
u saradnji sa Razvojnim programom Ujedinjenih nacija (UNDP)**

PRIJEDLOG PROGRAMA CJELOŽIVOTNOG UČENJA “SIGURNOST INFORMACIJA”

Voditelj:
Prof. dr. Saša Mrdović

1. Pravni osnov

Na osnovu člana 37. Zakona o visokom obrazovanju Kantona Sarajevo („Službene novine Kantona Sarajevo“, br. 36/22) i člana 45. i 154. Statuta Univerziteta u Sarajevu, Program cjeloživotnog učenja „Sigurnost informacija“ bit će organiziran kao zajednička aktivnost Centra za interdisciplinarne studije Univerziteta u Sarajevu – „prof. dr. Zdravko Grebo“ i Razvojnog programa Ujedinjenih nacija (UNDP)

Centar za interdisciplinarne studije – “prof. dr. Zdravko Grebo” (CIS) je podorganizaciona jedinica Univerziteta u Sarajevu koja ima za cilj promociju novih zahtjeva u sferi visokog obrazovanja i potrebu za kreiranjem programa koji prevazilaze okvire jedne naučne discipline. Trendovi u visokom obrazovanju, naučno istraživačkom radu i cjeloživotnom učenju podrazumijevaju povezivanje različitih disciplina, jer tržište rada i akademska zajednica zahtijevaju izlazak van okvira uskih profesija, kakvim smo najčešće izloženi. CIS je usmjeren ka interdisciplinarnom obrazovanju nove generacije stručnjaka/inja iz Bosne i Hercegovine kao i iz zemalja regije jugoistočne Evrope. Kao takav, CIS okuplja više od stotinu uvažanih domaćih i stranih eksperata i ekspertica iz različitih naučnih oblasti koji zajednički rade na projektima razvoja. Svoje mjesto CIS je našao u okviru Univerziteta u Sarajevu i predstavlja inovativni inkubator za interdisciplinarne programe.

Fokus djelovanja CIS-a bazira se na tri osnovna postulata, i to:

1. ciklično obrazovanje u vidu master i doktorskih studija,
2. neciklično obrazovanje u vidu kratkih programa cjeloživotnog učenja i
3. naučno-istraživački i tržišno orijentisani projekti interdisciplinarnog karaktera.

Memorandumom o razumijevanju između Razvojnog programa Ujedinjenih nacija (UNDP) i Univerziteta u Sarajevu od 23.12.2020. godine formalizirana je saradnja u području ciljeva postavljenih unutar UNDP-ovog državnog programa 2021-2025 koji su posebno usmjereni prema održivom i inkluzivnom rastu. Područja saradnje su inter alia:

- i) Zajedničko dizajniranje i provođenje obrazovnih inicijativa i inicijativa za učenje koje uključuje mlade ljude u inovativna razmišljanja i razmišljanja okrenuta budućnosti.
- ii) Saradnja u obogaćivanju nastavne ponude univerziteta iz perspektive Agende 2030 i ciljeva održivog razvoja, uključujući pilot programe učenja, gostujuće predavače itd.

Član I Memoranduma predviđa da je Centar za interdisciplinarne studije (CIS) Univerziteta u Sarajevu glavna tačka za provođenje odredbi memoranduma.

2. Trajanje i način izvođenja programa

Program Obuke „Sigurnost informacija“ će trajati ukupno 9 mjeseci.

Program cjeloživotnog učenja „Sigurnost informacija“ će se izvesti u periodu od 1.9.2024. do 15.5.2025. godine. Sve programske aktivnosti će se izvoditi u prostorijama CIS-a, te hibridno, upotrebom platformi za učenje i interakciju na daljinu koje koristi CIS.

3. Ciljna skupina

Program „Sigurnost informacija“ je namijenjen kandidatima/kinjama koji/e su:

- 1) Završili akademsko obrazovanje iz oblasti informatike ili imaju bar pet godina iskustva rada u ovoj oblasti;
- 2) Uposlenici na IKT poslovima državnih institucija sa svih nivoa vlasti u BiH (za prvu izvedbu obuke, uz moguće proširenje za buduće obuke).

Ciljna skupina je određena u skladu sa ciljevima programa.

4. Cilj programa

Cilj Obuke je obrazovati visoko kvalifikovane kadrove iz oblasti sigurnosti informacija. Ti kadrovi trebaju postati tehnički i organizacioni voditelji u oblasti sigurnosti informacija. Ovi kadrovi će biti u stanju projektovati zaštite prilagođene potrebama i mogućnostima organizacije, a usklađene sa međunarodnim standardima i najboljim praksama. Oni će moći preuzeti složene specijalističke poslove iz oblasti sigurnosti informacija. Da bi se ovo ostvarilo, steći će šire interdisciplinarno obrazovanje koje pored tehničkog uključuje i društvene, ekonomske i pravne aspekte sigurnosti informacija.

5. Opis programa

Savremeni narativ je da živimo u informacionom dobu. Informacije su osnova na kojoj odnosimo odluke, kako poslovne tako i privatne. Ova činjenica čini sigurnost informacija jako bitnom. Sigurnost informacija se ostvaruje kroz njihovu povjerljivost, cjelovitost i dostupnost. Povjerljivost je ostvarena ako su informacije dostupne samo onim kojima trebaju biti. Cjelovitost je ostvarena ako se informacije ne mogu neovlašteno izmijeniti bez otkrivanja. Cjelovitost je ostvarena ako su informacije dostupne onima kojima trebaju i kada trebaju. Današnja obrada informacija se pretežno radi kroz računarske sisteme pa se nerijetko povezuje isključivo sa računarstvom i informatikom. Kako bi se sagledala šira slika uticaja sigurnosti informacija na društvo, neophodan je interdisciplinarni pristup.

Obrazovanje IKT i ostalih kadrova o zaštiti informacija se može smatrati kao jedna od najznačajnijih mjera koje dugoročno mogu dati pozitivne rezultate u kontekstu smanjenja rizika od njihove zloupotrebe. Obrazovanje o važnosti očuvanja sigurnosti informacija, o uticaju ponašanja korisnika i IKT profesionalaca, mjerama prevencije, detekcije i korekcije,

povećanju zaštitnih kapaciteta i otpornosti društva i pojedinca kroz planske mjere i aktivnosti, igra ključnu ulogu u izgradnji sigurnog društva.

Program “Sigurnost informacija” kroz svoj sadržaj nudi interdisciplinarni pristup u analizi i izučavanju ove problematike. Kroz nastavni proces, interaktivne radionice, edukacijske kvizove i ciljna istraživanja potpomognuta mentorima će se prije svega postići podizanje znanja i svijesti o ovim izazovima, razumijevanju uzroka i posljedica ugrožavanja sigurnosti informacija, te poticanje kritičkog promišljanja i održivog ponašanja, kao i poticanja na izgradnju mjera prevencije i zaštite informacija i društva u cjelini.

6. Ishodi učenja

Po uspješno završenom Programu polaznik će steći sljedeća znanja, vještine i kompetencije:

Znanja:

- Definiše neophodne tehnike i prakse usklađene sa standardima i procedurama sigurnosti informacija;
- Radi tehničku validaciju sigurnosnih alata;
- Predlaže rješenja za sigurnu integraciju kritičnih poslovnih procesa;
- Analizira rizike i prijetnje po sigurnost informacija.

Vještine:

- Sprovodi neophodne tehnike i prakse sigurnosti informacija;
- Stavlja u upotrebu, konfigurira i koristi odgovarajuće alate;
- Provodi politiku sigurnosti informacija organizacije odgovarajućom upotrebom IKT resursa;
- Identificira i otklanja sigurnosne propuste.

Kompetencije:

- Doprinosi sigurnosnim praksama, osviještenosti i usklađenosti davanjem savjeta, podrške, informacija i obuke;
- Nadzire dešavanja u oblasti sigurnosti da osigura efikasnost i efektivnost procesa i kontrola informacione sigurnosti.

7. Metode rada

Program se realizira kroz 11 kurseva, od toga deset kurseva sa po 30 i jedan sa 15 sati nastave. Nastava se odvija na bosanskom/hrvatskom/srpskom jeziku. Program će trajati 9 mjeseci. Kursevi će se odvijati modularno, svaki u trajanju od tri sedmice. Svaki od kurseva sadrži jednu oblast.

8. Uslovi za prijavu

Polaznike na Program „Sigurnost informacija“ će, odrediti i izabrati nadležne agencije za državnu službu. One će to uraditi kroz svoje procese koordinacije sa državnim institucijama iz njihove nadležnosti.

9. Troškovi

Potrebne troškove angažmana nastavnog osoblja, kao i smještaja i putovanja nastavnog osoblja i polaznika Obuke pokriva UNDP BiH.

10. Kursevi

Naziv kursa	Izazovi u međunarodnoj i regionalnoj sigurnosti
Ciljevi	<p>Upoznavanje polaznika kursa sa temeljnim pitanjima sigurnosti, kako im pomoglo da razviju napredno razumijevanje savremenog sigurnosnog okruženja. Sigurnost informacija je dio sveukupne sigurnosti. Šire razumijevanje ove problematike je dobar uvod prije fokusiranja na sigurnost informacija. Upoznavanje polaznika kursa sa temeljnim temama i alatima razvijenim za analizu sigurnosnih izazova na međunarodnom i regionalnom nivou. Polaznici će se oslanjati na različite teorijske pristupe, od kojih mnogi proširuju ideje i teme obuhvaćene u temeljima međunarodne i regionalne sigurnosti, kako bi istražili savremene sigurnosne izazove i diskurse o sigurnosti/nesigurnosti. Kurs će poboljšati njihove analitičke vještine za procjenu sigurnosnih izazova i za izgradnju nezavisnih istraživačkih strategija koje im omogućuju da razviju originalne argumente o novim i trajnim sigurnosnim žarištima. Ovi koncepti se provlače kroz sve kurseve, i aspekte, sigurnosti informacija. Ovaj kurs pokriva napredne načine analize novih ili složenih sigurnosnih izazova, pri čemu razvoj tradicionalnih i kritičkih učenja igra svoju ulogu.</p>
Ishodi učenja	<p>Po uspješnom završetku kursa student će moći:</p> <ul style="list-style-type: none">• Pokazati razumijevanje izazova regionalne i međunarodne sigurnosti i izvora kriza i sukoba;• Procijeniti konkurentske tvrdnje i donijeti objektivne prosudbe o ulozi i utjecaju državnih i nedržavnih aktera na međunarodnu sigurnosnu agendu;• Pokazati temeljito poznavanje i kritičko razumijevanje novije literature i povezati njezine argumente sa savremenim sigurnosnim izazovima;• Unaprijediti sposobnost specijaliziranja u dubinskom poznavanju određenog regionalnog aktera i analiziranju njegovog značaja i stava o nizu regionalnih i međunarodnih sigurnosnih pitanja;• Proširiti vještine komuniciranja u pisanom i usmenom obliku o glavnim pitanjima međunarodne i regionalne sigurnosti.• Prezentirati jasne, analitičke i snažne argumente u pisanom i usmenom obliku

Naziv kursa	Osnove sigurnosti informacija
Ciljevi	Upoznavanje studenata sa osnovnim pojmovima i konceptima vezanim za sigurnost informacija. Ovi koncepti se provlače kroz sve kurseve, i aspekte, sigurnosti informacija.
Ishodi učenja	<p>Po uspješnom završetku kursa student će moći:</p> <ul style="list-style-type: none"> • Objasniti globalni uticaj sigurnosti informacija na društvo, uključujući oblasti kao što su ekonomija, socijalna pitanja, politika i zakoni; • Objasniti i primijeniti koncepte povjerljivosti, cjelovitosti i dostupnosti informacija; • Objasniti koncepte povjerenja i pouzdanosti; • Objasniti šta je politika sigurnosti informacija i njenu ulogu u zaštiti podataka i resursa; • Objasniti, diskutovati i primijeniti različite načine potvrđivanja identiteta (<i>authentication</i>); • Objasniti, diskutovati i primijeniti različite načine provjere ovlaštenja (<i>authorization</i>); • Opisati upravljanje rizicima i njegovu ulogu u organizaciji; • Opisati i analizirati rizik po sigurnost informacija; • Analizirati sigurnost informacija iz ugla napadača; • Diskutovati o različitim motivima ponašanja u oblasti cyber kriminala; • Navesti zakone relevantne za sigurnost informacija u BiH i regionu; • Poznavati EU direktive i druge regulative iz oblasti sigurnosti informacija; • Ocijeniti usklađenost organizacije sa izabranim zakonom ili direktivom; • Razviti sistemski pristup sigurnosti informacija koji uključuju društvene i tehničke aspekte.

Naziv kursa	Ljudski faktor
Ciljevi	Naučiti o napadima na sigurnost informacija preko ljudi i njihovog ponašanja, kao i odbranama od ovih napada.
Ishodi učenja	<p>Po uspješnom završetku kursa student će moći:</p> <ul style="list-style-type: none"> • Analizirati posebnosti ljudi i njihovog ponašanja bitne za sigurnost informacija; • Pokazati razumijevanje različitih napada društvenog inženjeringa, psihologiju ovih napada i zbunjivanja korisnika; • Pokazati sposobnost da provede mjere za otkrivanje i zaustavljanje napada društvenog inženjeringa; • Diskutovati važnost <i>cyber</i> higijene, obrazovanja korisnika o sigurnosti informacija i svjesnosti o sigurnosnim ranjivostima i prijetnjama. • Objasniti važnosti zaštite ličnih podataka i privatnosti i propise koji regulišu ovu oblast; • Objasniti najčešće vrste ugrožavanja privatnosti; • Diskutovati o važnosti privatnosti i sigurnosti na društvenim mrežama; • Opisati zašto su etički kodeksi ponašanja važni za profesionalce u oblasti sigurnosti informacija i njihove organizacije;

Naziv kursa	Standardi i metodologije sigurnosti informacija
-------------	---

Ciljevi	Cilj je razvijanje razumijevanja važnosti standarda i metodologija za zaštitu sigurnosti informacija. Osposobljavanje studenata za analizu usklađenosti sustava s relevantnim standardima, primjenu metodologija za efikasno upravljanje sigurnošću, te razvijanje i uspostavljanje sigurnosnih sustava u skladu s odabranim standardima. Studenti će naučiti predlagati strategije za poboljšanje sigurnosnih praksi i provoditi kontinuirano praćenje i evaluaciju sigurnosnih sistema kako bi se prilagodili promjenjivim okolnostima i prijetnjama.
Ishodi učenja	Po uspješnom završetku kursa student će moći: <ul style="list-style-type: none"> • Objasniti važnost standarda i metodologija za zaštitu sigurnosti informacija; • Navesti najvažnije međunarodne standarde i metodologije iz oblasti; • Analizirati usklađenost nekog sistema sa izabranim standardom; • Primijeniti izabranu metodologiju za ostvarivanje sigurnosti informacija; • Uspostaviti sistem koji je usklađen sa izabranim standardom.

Naziv kursa	Sigurnost softvera
Ciljevi	Naučiti principe i metode razvoja sigurnog softvera, razviti sposobnost identifikacije i analize sigurnosnih prijetnji i ranjivosti kroz različite faze razvoja. Primjenjivati tehnike i metode za osiguravanje sigurnosti koda, koristiti specijalizirane alate za testiranje sigurnosti, te razvijati strategije za upravljanje sigurnosnim incidentima. Fokus će biti i na razumijevanju pravnih i etičkih aspekata sigurnosti softvera, te na razvoju vještina potrebnih za efikasnu komunikaciju sigurnosnih izazova i rješenja unutar organizacija i prema vanjskim sudionicima. Sve ovo studentima će omogućiti da postanu stručnjaci koji mogu proaktivno djelovati na zaštiti softvera i podataka u dinamičnom tehnološkom okruženju.
Ishodi učenja	Po uspješnom završetku kursa student će moći: <ul style="list-style-type: none"> • Razvijati softver koristeći sigurni životni ciklus razvoja; • Objasniti zašto su sigurnosni zahtjevi važni; • Identificirati zajedničke vektore napada; • Opisati važnost pisanja sigurnih i robusnih programa; • Objasniti zašto je validacija ulaznih podataka neophodna; • Razlikovati sigurno kodiranje i zakrpe i objasniti prednost korištenja sigurnih tehnika kodiranja; • Opisati preljev međuspremika (<i>buffer overflow</i>) i zašto je to potencijalni sigurnosni problem; • Razlikovati statičku i dinamičku analizu; • Diskutovati o problemu koji statička analiza ne može otkriti; • Diskutovati o problemu koji dinamička analiza ne može otkriti; • Razgovarati o potrebi ažuriranja softvera radi otklanjanja sigurnosnih propusta; • Objasniti važnost pravilnog konfigurisanja softvera; • Napraviti procedure testiranja sigurnosti softvera; • Diskutovati o etičkim pitanjima u otkrivanju ranjivosti.

Naziv kursa	Sigurnost umrežavanja
Ciljevi	Naučiti sigurnosne izazove umrežavanja i kako ih prevladati.
Ishodi učenja	Po uspješnom završetku kursa student će moći: <ul style="list-style-type: none"> • Pokazati široko znanje o principima i praksi savremene sigurnosti mreže i komunikacija; • Objasniti i primijeniti koncepte nadzora i filtriranja mrežnog saobraćaja; • Objasniti i primijeniti koncepte detekcije upada u računarske mreže; • Analizirati posebnosti osiguravanja bežičnih komunikacija; • Procijeniti uticaj savremenih trendova umrežavanja na sigurnost (SDN, <i>cloud</i>, IoT).

Naziv kursa	Kriptografija
Ciljevi	Upoznati sa osnovama kriptografije i njenom ulogom u zaštiti sigurnosti informacija.
Ishodi učenja	Po uspješnom završetku kursa student će moći: <ul style="list-style-type: none"> • Opisati ulogu kriptografije u podršci sigurnosti i privatnosti informacija; • Opisati opasnosti od izmišljanja sopstvenih kriptografskih metoda; • Opisati ulogu kriptografije u podršci poverljivosti i privatnosti; • Napraviti izvedbu i kripto-analizu klasičnih šifratora; • Opisati moderne simetrične sisteme šifriranja i načine za njihovu kriptooanalizu; • Opisati moderne asimetrične (sa javnim ključem) sisteme šifriranja i načine za njihovu kriptooanalizu; • Uporediti različite algoritme u njihovoj podršci za sigurnost informacija; • Objasniti protokole razmjene ključeva i pokazati pristupe za smanjenje mogućnosti njihovog neuspjeha; • Opisati stvarne primjene kriptografskih primitiva i protokola; • Opisati kvantnu kriptografiju i uticaj kvantnog računarstva na kriptografske algoritme.

Naziv kursa	Digitalna forenzika
Ciljevi	Naučiti kako se provodi digitalna forenzička istraga, šta su njeni zadaci, kakve su procedure i alati koji se koriste.
Ishodi učenja	Po uspješnom završetku kursa student će moći: <ul style="list-style-type: none"> • Objasniti šta je digitalna istraga i kako se može sprovesti; • Opisati zakonske zahtjeve za korištenje zaplijenjenih podataka i njihovu upotrebu; • Opisati i sprovesti lanac čuvanja podataka od početne zaplijene digitalnih dokaza do njihove dispozicije; • Izvući podatke sa medija za pohranu u skladu sa zakonom; • Opisati profesionalnu odgovornost i odgovornost osobe prilikom svjedočenja kao forenzičar; • Povratiti podatke na osnovu zadanog termina za pretragu iz slike (<i>image</i>) sistema;

	<ul style="list-style-type: none"> • Rekonstruisati podatke i događaje iz historije aplikacije, web artefakta, baze podataka u oblaku ili mobilnog uređaja; • Snimiti i protumačiti mrežni saobraćaj; • Diskutovati o izazovima vezanim za forenziku mobilnih uređaja; • Primijeniti forenzičke alate za istraživanje narušavanja sigurnosti; • Identificirati i zaobići antiforenzičke metode.
--	--

Naziv kursa	Sigurnost web aplikacija
Ciljevi	Naučiti posebne opasnosti vezane za web aplikacije i kako se od njih zaštititi.
Ishodi učenja	<p>Po uspješnom završetku kursa student će moći:</p> <ul style="list-style-type: none"> • Razumjeti i objasniti posebnosti web aplikacija u odnosu na aplikacije na uređaju sa aspekta sigurnosti; • Objasniti različite načine čuvanja stanja kod web aplikacija; • Opisati različite vrste napada na web aplikacije; • Objasniti potrebu provjere ulaznih podataka na strani servera; • Opisati moguće napade na mehanizme čuvanja stanja web aplikacija (<i>cookie</i>, JWT); • Objasniti različite napade umetanja koda; • Predložiti i provesti zaštite od napade umetanja koda; • Objasniti različite XSS napade; • Predložiti i provesti zaštite XSS napada; • Analizirati sigurnost neke web aplikacije; • Predložiti i provesti zaštite neke web aplikacije.

Naziv kursa	Sigurnost baza podataka
Ciljevi	Naučiti zaštititi baze podataka.
Ishodi učenja	<p>Po uspješnom završetku kursa student će moći:</p> <ul style="list-style-type: none"> • Uporediti sigurnosne arhitekture baza podataka radi po pogodnosti za stvaranje sigurnog okruženja za rad; • Objasniti zaštitne mehanizme sigurnosti informacija koje imaju različite baze podataka; • Koristiti dostupne mehanizme za izvedbu i održavanje sigurnosti informacija u bazi podataka; • Osmisliti, izvesti testirati i dokumentovati sigurne aplikacije baze podataka.

Naziv kursa	Obrada incidenata
Ciljevi	Naučiti šta raditi u slučaju sigurnosnog incidenta i kako minimizirati njegov negativni učinak.
Ishodi učenja	<p>Po uspješnom završetku kursa student će moći:</p> <ul style="list-style-type: none"> • Razumjeti proces obrade incidenata; • Razumjeti pravne, ljudske i poslovne posljedice incidenta; • Definisati indikatore koji ukazuju na incident; • Dizajnirati sistem za nadzor koji će otkrivati incidente na osnovu indikatora;

	<ul style="list-style-type: none">• Objasniti ulogu različitih učesnika u obradi incidenata;• Osmisliti, uspostaviti i sprovesti proceduru za obradu incidenata;• Osmisliti, uspostaviti i sprovesti proceduru obavještanja u slučaju incidenata;• Osmisliti, uspostaviti i sprovesti proceduru oporavka od katastrofalnog događaja;• Osmisliti, uspostaviti i sprovesti proceduru očuvanja kontinuiteta poslovanja;• Sačuvati podatke potrebne za provođenje forenzičke istrage;• Razumjeti i naučiti iz većih incidenata koji su se desili u skorijoj prošlosti;
--	--

Univerzitet u Sarajevu



University of Sarajevo



CIS Centar za interdisciplinarne studije
Univerziteta u Sarajevu
prof. dr. Zdravko Grebo



CERTIFIKAT

kojim se potvrđuje da je

(ime i prezime polaznika)

uspješno završio/la _____.

(naziv programa).

Program je odobren Odlukom Senata Univerziteta u Sarajevu broj ___od___,
struktura i ishodi Programa su opisani u dodatku certifikata.

Datum:

Broj:

DIREKTOR

Centra za interdisciplinarne studije – „prof. dr. Zdravko Grebo“

M.P

VODITELJ PROGRAMA
