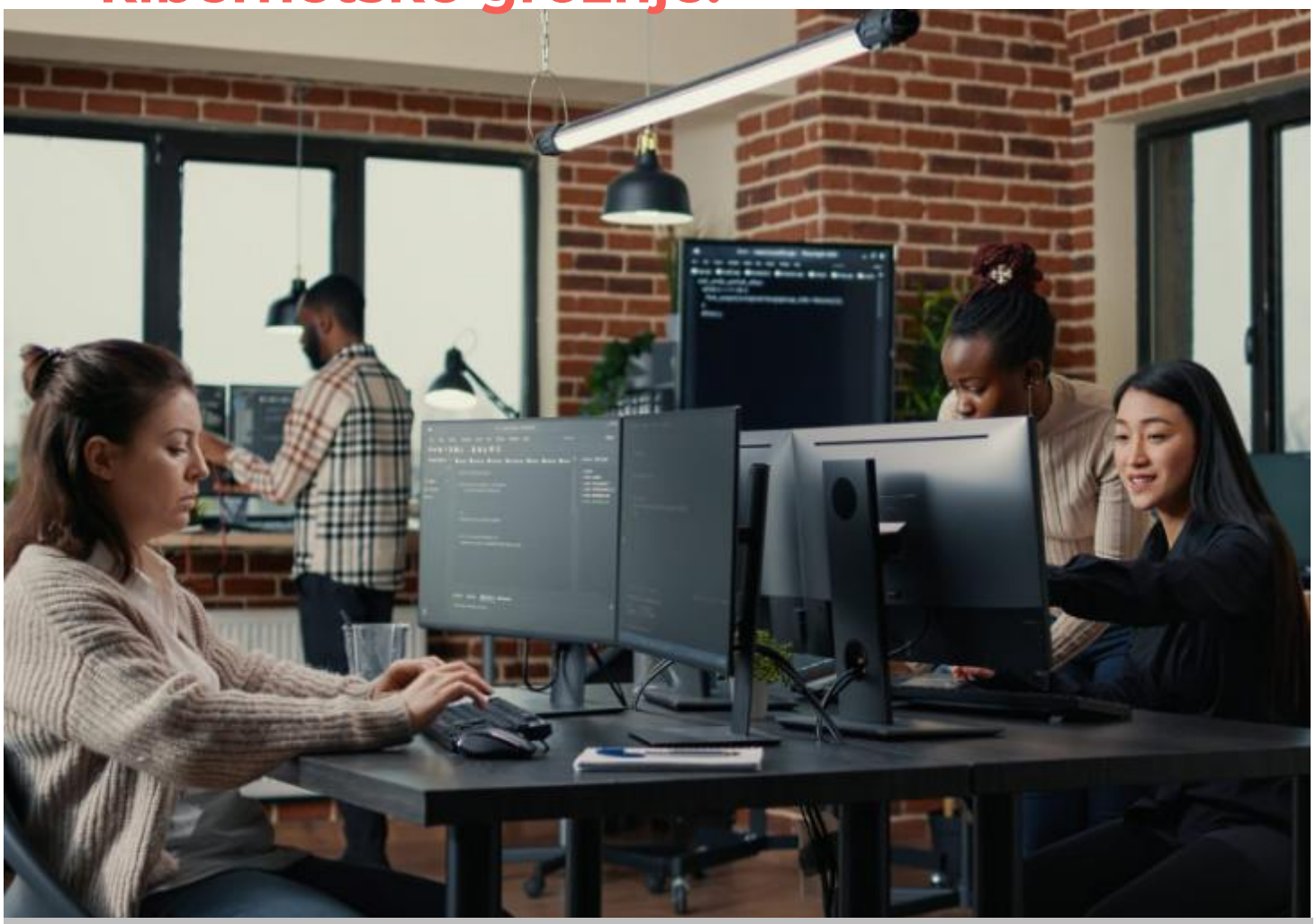
Naučite se prepoznati, preprečiti in odzvati se na sodobne kibernetske grožnje.



SRIP GoDigital zit SeKV CyberHub Slovenia DIGI-SI

Ponovitveni cikel akademije kibernetske varnosti

Brezplačna akademija kibernetske varnosti v obsegu 4 seminarjev v izvedbi Fakultete za elektrotehniko, računalništvo in informatiko (UM FERI)

Trajanje : med 24. 8. 2026 in 30. 9. 2026

Akademija kibernetske varnosti

Zakaj akademija kibernetske varnosti

V današnjem digitaliziranem svetu je kibernetska varnost postala ključnega pomena. V poslovnem svetu predstavlja kibernetska varnost strošek, ki je lahko upravičen le, če preprečuje še višje stroške, ki bi nastali brez teh vlaganj. Zaradi predpisnih zahtev, potencialne izgube ugleda organizacije in komercializacije napadov, je razmerje med stroški in koristjo kibernetske varnosti strmo narastlo v prid uporabi učinkovite zaščite in sodelovanju IKT strokovnjakov s področja kibernetske varnosti. Eurobarometer poroča, da 45 % podjetij navaja **težave pri iskanju osebja** z ustreznimi znanji kot enega glavnih izzivov s področja kibernetske varnosti.

Potrebe po strokovnjakih s kompetencami na področju kibernetske varnosti strmo naraščajo tako pri vseh organizacijah, kot tudi pri ponudnikih in proizvajalcih rešitev in storitev informacijske tehnologije. Vsak košček digitalnih rešitev in storitev mora biti načrtovan in narejen z mislijo na kibernetsko varnost. Izobraževalni sistem in trg dela ne sledita naraščajočim potrebam po kibernetski varnosti, zato je izrednega pomena čim prej nasloviti naraščajočo vrzel. EU in tudi države članice pripravljajo različne ukrepe in programe za vse življenjsko učenje, ki bodo zaposlenim omogočili tako posodabljanje znanja, kot tudi prekvalifikacije.

Fakulteta za elektrotehniko, računalništvo in informatiko, Univerze v Mariboru (UM FERI) sodeluje v projektu EDIH DIGI-SI, »European Digital Innovation Hub Slovenija«, ki v okviru evropske mreže EDIH podpira digitalno preobrazbo podjetij in organizacij javnega sektorja. Med pomembnimi področji projekta so tudi krepitev digitalnih kompetenc, uvajanje naprednih digitalnih tehnologij in kibernetska varnost. V tem okviru se Akademija kibernetske varnosti umešča med aktivnosti, namenjene pridobivanju praktičnih znanj za varnejše in učinkovitejše digitalno poslovanje.

UM FERI, CyberHub Slovenija, SRIP GoDigital, EDIH DIGI-SI in Združenje za informatiko in telekomunikacije s Sekcijo za kibernetsko varnost vas vabimo, da se udeležite ponovitve uspešne **Akademije kibernetske varnosti**, ki je sestavljena iz **štirih seminarjev**, s katerimi boste pridobili znanja iz izbranih področij kibernetske varnosti.

Vabimo vas, da izkoristite to **priložnost** in se nam pridružite na izobraževanjih, na katerih boste imeli priložnost razširiti svoje znanje in veščine iz kibernetske varnosti. Akademija se izvaja že **tretje leto**, zato imate priložnost, da se udeležite tudi tistih seminarjev, ki ste jih morda lani zamudili. Hkrati ponujamo letos tudi nov seminar, in sicer »**Ai in kibernetska varnost**«. Več o vsebini posameznih seminarjev akademije si lahko preberete v nadaljevanju.

Vsebina akademije kibernetske varnosti

Seminarji, vključeni v akademijo kibernetske varnosti, pokrivajo različna področja kibernetske varnosti. **Spletna varnost in vdorno testiranje** sta v veliki meri dve strani istega kovanca, kjer se ena stran ukvarja z oblikami varovanja, medtem ko druga izkorišča prisotne ranljivosti oz. pomanjkljivosti (predvidoma za namene izboljšanja varnosti). Seminar **Identifikacija, overjanje in avtorizacija** se osredotoča na temeljne koncepte IAA ter različne modele digitalnih identitet – od silosnih in centraliziranih do federativnih in decentraliziranih pristopov. Poudarek bo na praktičnih metodah overjanja, infrastrukturi javnih ključev, digitalnih potrdilih ter protokolih. Udeleženci bodo spoznali tudi večfaktorsko overjanje, modele avtorizacije in njihovo uporabo v sodobnih IT okoljih. **AI in kibernetska varnost** bo ponudila vse ključne informacije o tem, kako lahko uporabimo umetno inteligenco kot podporo pri zagotavljanju informacijske varnosti, kakor tudi informacijsko-varnostne pasti, ki jih srečamo ob uporabi umetne inteligence. **Upravljanje informacijske varnosti** je zahtevna in kompleksna naloga, ki jo morajo naslavljati vse (večje) organizacije, česar se morajo zavedati predvsem vodstveni kadri. Izobraževanje bo predstavilo osnovne problematike in naslovilo pristope upravljanja za zagotovitev smiselnega varovanja zaupnosti, celovitosti in dostopnosti sredstev organizacije pred potencialnimi grožnjami.

Lokacija akademije kibernetske varnosti

Akademija je sestavljena iz štirih seminarjev, od katerih vsak pokriva svoje področje. Enodnevni seminarji potekajo v živo, **v Ljubljani (GZS)**, na **Dimičevi ulici 13, v dvorani E** in **F** (medetaža) po spodnji razporeditvi.

»Spletna varnost in vdorno testiranje«: 24. 8. 2026, 09:00–16:30, Dvorana F
»Identifikacija, overjanje in avtorizacija«: 7. 9. 2026, 09:00–16:30, Dvorana E
»AI in kibertnetska varnost«: 21. 9. 2026, 09:00–16:30, Dvorana F
»Upravljanje informacijske varnosti«: 30. 9. 2026, 09:00–16:30 Dvorana E

Pogoji udeležbe

- Udeležiti se je mogoče poljubnega nabora seminarjev, vendar se v primeru prevelikega števila prijav daje prednost tistim, ki izberejo večje število seminarjev.
- Da se seminar izvede je potrebno minimalno 10 udeležencev.
- Za zagotovitev pogojev, ki so potrebni za kakovostno izvedbo seminarjev, je število udeležencev omejeno na maksimalno 20.
- Potrebno predznanje je opredeljeno v okviru opisa seminarjev.

Kotizacija in prijave na akademijo kibernetske varnosti

Izvedba seminarjev, ki so vključeni v akademijo kibernetske varnosti, poteka v sklopu EDIH DIGI-SI 2 in je brezplačna za člane ZIT, SRIP GoDigital in člane GZS.

Seminarji bodo potekali na **GZS, Dimičeva ulica 13** (Ljubljana), **v dvorani E** in **F** – (medetaža) po spodnji razporeditvi. **Za posamezni seminar se je potrebno prijaviti ločeno**, prijave lahko najdete na tej povezavi.

Prijave in potek posameznih seminarjev lahko najdete spodaj:

SEMINAR 1: 24. 8. 2026, 09:00 – 16:30, Dvorana F – PRIJAVA TUKAJ
SEMINAR 2: 7. 9. 2026, 09:00 – 16:30, Dvorana E – PRIJAVA TUKAJ
SEMINAR 3: 21. 9. 2026, 09:00 – 16:30, Dvorana F – PRIJAVA TUKAJ
SEMINAR 4: 30. 9. 2026, 09:00 – 16:30, Dvorana E – PRIJAVA TUKAJ

Rok za prijavo je 24. 07. 2026.
Neudeležbo na posameznem seminarju bomo zaračunali v višini 150 € + DDV.

Utrinki preteklih let

V nadaljevanju predstavljamo nekaj utrinkov z Akademije kibernetske varnosti iz preteklih izvedb.

Odzivi in vtisi preteklih udeležencev:

»Predavanja so bila super. Ni bilo branja s prosojnic ampak govorjenje na pamet!!! Odlično!«

»Hvala za vaš trud, vse je bilo na zelo visokem nivoju, od organizacije do vsebin. Všeč mi je bila uravnoteženost med teorijo in prakso, čeprav je bilo za nas z manj študijske kondicije kar naporno.«

»Všeč so mi t.i. \"real life scenarios\" - kar ste tudi demonstrirali na tem šolanju in upam, da ne spremenite tega modela podajanja informacij. Dobiti stik z osebami, ki dejansko v praksi izvajajo te aktivnosti je bilo zelo poučno.«

SEMINAR 1: Spletna varnost in vdorno testiranje

Predavatelj: izr. prof. dr. Marko Hölbl (UM FERI) in izr. prof. dr. Muhamed Turkanović (UM FERI)
Datum, čas in lokacija: 24. 8. 2026, 09:00 – 16:30, dvorana F

Kratek opis:
V okviru izobraževanja bodo udeleženci spoznali področje spletne varnosti in vdornega (penetracijskega) testiranja. Predstavljena bodo načela etičnega hekanja ter s tem povezane faze etičnega hekanja, procesi, orodja in ogrodja za izvedbo le tega. Fokus bo vdorno testiranje, povezano s spletnimi aplikacijami, pri čemer pa bo predstavljeno tudi izvidništvo, skeniranje omrežja, sistemsko vdiranje, itn.
V drugem delu bodo predstavljena načela spletne varnosti z vidika odjemalca, strežnika in komunikacijske povezave. Kot eden ključnih vidikov spletne varnosti bo obravnavan spletni varnostni model in njegovi gradniki (SOP, CSP, SRI, CORS), ki zagotavlja varnost na strani odjemalca. Prav tako bo predstavljen strežniški del spletne varnosti preko seznama najbolj pogostih ranljivosti (OWASP Top 10). Pri tem bodo obravnavane omenjene ranljivosti in kako se pred njimi zaščititi. Del izobraževanja bo tudi namenjen mehanizmom varovanja komunikacijske povezave med strežnikom in odjemalcev, kar je mogoče s pomočjo varnostnega protokola HTTPS in ustreznega upravljanja sej.

Izobraževanje je namenjeno posameznikom, ki bi radi pridobili/nadgradili znanja s področja celovite spletne varnosti in vdornega testiranja, ki predstavljata dopolnjujoči se temi kibernetske varnosti.

Želena predznanja in oprema:.
Priporočljivo osnovno poznavanje tehnologij, ki jih bomo uporabljali: HTML, CSS, JavaScript, SQL ipd.
Osnovno znanje računalniških omrežij
Osnovno znanje programiranja

Po zaključku izobraževanja bo udeleženec sposoben:
- razumeti mehanizme, metode in protokole za zaščito spletih aplikacij, spletni varnosti model in varovanje komunikacijske povezave
- razumeti tipično spletno infrastrukturo in načine napadov
- opisati faze etičnega hekanja
- opisati etične in pravne posledice etičnega hekanja
- načrtovati vdorni test
- opisati orodja namenjenega vdornemu testiranju in njihove glavne zmogljivosti

SEMINAR 2: Identifikacija, overjanje in avtorizacija

Predavatelj: izr. prof. dr. Muhamed Turkanović (UM FERI), Vid Keršič (UM FERI)
Datum, čas in lokacija: 7. 9. 2026, 09:00 – 16:30, dvorana E

Kratek opis:
Izobraževanje bo zajemalo osrednje koncepte identifikacije, overjanja in avtorizacije (ang. Identification, authentication and authorization – IAA), pri čemer bomo začeli z uvodom v IAA, ključnimi koncepti in terminologijo. Raziskali bomo modele digitalnih identitet, vključno s silosnimi, centraliziranimi, federativnimi in decentraliziranimi pristopi, ter primere uporabe posameznih modelov. Nadaljevali bomo z metodami identifikacije in overjanja, kot so gesla, PIN kode, žetoni, pametne kartice, biometrija, ter overjanje na nivoju mobilnih in spletnih rešitev.
V okviru infrastrukture bomo pokrili infrastrukturo javnih ključev, X.509 certifikate, kvalificirana in nekvalificirana digitalna potrdila ter ponudnike digitalnih identitet, kot so federativno poslovni ali Google in Microsoft. V implementaciji overjanja bomo raziskali protokole in standarde, kot so OAuth2.0, OpenID Connect in SAML, ter upravljanje sej s pomočjo JWT žetonov. Poudarek bo tudi na več faktorskem overjanju z uporabo WebAuthn in FIDO2/U2F. Avtorizacijo in nadzor dostopa bomo obravnavali skozi ogrodja RBAC in ABAC ter implementacijo v sodobnih IT arhitekturah, vključno z mikrostoritvami in spletnimi storitvami. V zadnjem delu izobraževanja se bomo posvetili praktičnim aplikacijam in prihajajočim tehnologijam, kot so decentralizirane in samo-upravljane identitete, podprte z verigami blokov, ter digitalne denarnice in uredbe, kot je eIDAS 2.0.
To izobraževanje bo udeležencem omogočilo celovit vpogled v identifikacijo, overjanje in avtorizacijo, ter jih opremilo s praktičnimi znanji za učinkovito upravljanje digitalnih identitet in izboljšanje kibernetske varnosti.

Izobraževanje je namenjeno posameznikom, ki bi radi pridobili/nadgradili znanja za potrebe »full stack« razvijalca spletnih aplikacij, kjer bodo razvili zaledne komponente interaktivne spletne aplikacije na poljubno izbrani problemski domeni.

Želena predznanja:
- Osnovno razumevanje tehnologij svetovnega spleta (npr. HTTP, HTML, CSS)
- Poznavanje sistemov za nadzor verzij (npr. git) in platform (npr. GitHub)
- Poznavanje vsaj enega objektno usmerjenega programskega jezika (priporočljivo JavaScript)
- Osnovno poznavanje okolij/orodij, ki jih bomo uporabljali: Node.js, MongoDB, Docker, Visual Studio Code
-

Po zaključku izobraževanja bo udeleženec sposoben:
- razumeti koncepte digitalne identitete, overjanja in avtorizacije
- razpravljati o prednostih in slabostih različnih metod overjanja
- razumeti, kako izbrati najprimernejšo metodo overjanja,
- opisati in primerno uporabiti tehnologije za upravljanje identitet ter zagotavljanje overjanja
- izvajati in upravljati varno overjanje z uporabo protokolov in standardov, kot so OAuth2.0, OpenID Connect, SAML, ter upravljati seje s pomočjo JWT žetonov

SEMINAR 3: AI in kibernetska varnost

Predavatelj: Maja Rotovnik (UM FERI), Nika Jeršič (UM FERI), izr. prof. dr. Marko Hölbl (UM FERI)
Datum, čas in lokacija: 21. 9. 2026, 09:00 – 16:30, dvorana F

Kratek opis:
Izobraževanje AI in kibernetska varnost bo ponudilo vpogled v povezavo med umetno inteligenco in sodobno kibernetsko varnostjo. Udeleženci bodo spoznali, kako lahko umetno inteligenco uporabimo kot podporo pri zagotavljanju informacijske varnosti, kakor tudi tveganja in varnostne pasti, ki jih prinaša uporaba sistemov umetne inteligence.
V prvem delu izobraževanja bodo predstavljeni osnovni koncepti umetne inteligence, strojnega učenja in generativne umetne inteligence ter njihova uporaba pri zaznavanju napadov in obrambi (npr. anomalij, analizi dnevniških zapisov, odkrivanju zlonamerne programske opreme, …). Obravnavana bo tudi uporaba velikih jezikovnih modelov (LLM) pri avtomatizaciji varnostnih procesov ter podpori pri etičnem hekanju in vdornem testiranju.
V drugem delu bodo predstavljeni varnostni in etični izzivi uporabe umetne inteligence, vključno z napadi na modele strojnega učenja, zastrupljanjem podatkov, prompt injection napadi, uhajanjem informacij ter tveganji pri uporabi generativne umetne inteligence v organizacijah. Obravnavani bodo tudi regulativni in pravni vidiki ter dobre prakse za varno uporabo AI rešitev.
Izobraževanje je namenjeno posameznikom, ki bi radi pridobili ali nadgradili znanja s področja uporabe umetne inteligence v kibernetski varnosti ter razumeli tveganja, ki jih umetna inteligenca predstavlja za sodobna digitalna okolja.

Izobraževanje je namenjeno posameznikom, ki bi radi pridobili ali nadgradili znanja s področja uporabe umetne inteligence v kibernetski varnosti ter razumeli tveganja, ki jih umetna inteligenca predstavlja za sodobna digitalna okolja.

Želena predznanja:
- Osnovno poznavanje konceptov informacijske in kibernetske varnosti.
- Osnovno razumevanje delovanja umetne inteligence in strojnega učenja.
- Osnovno znanje programiranja in spletnih tehnologij je priporočljivo.
- Na dan vaj bodo udeleženci potrebovali tudi lastne prenosnike.

Po zaključku izobraževanja bo udeleženec sposoben:
- razumeti temeljne koncepte umetne inteligence in njihove uporabe v kibernetski varnosti
- opisati načine uporabe umetne inteligence za zaznavanje in obvladovanje varnostnih incidentov
- prepoznati tveganja in ranljivosti sistemov umetne inteligence
- razumeti najpogostejše napade na AI sisteme in načine zaščite pred njimi
- oceniti varnostne in etične vidike uporabe generativne umetne inteligence v organizacijah
- uporabljati dobre prakse za varno uporabo umetne inteligence v sodobnih informacijskih sistemih

SEMINAR 4: Upravljanje informacijske varnosti

Predavatelj: doc. dr. Lili Nemec Zlatolas in doc. dr. Marko Kompara
Datum, čas in lokacija: 30. 9. 2026, 09:00 – 16:30, dvorana E

Kratek opis:
Seminar upravljanja informacijske varnosti je osnovan na podlagi in vključuje vsebine, potrebne za ISACA certifikat CISM (Certified Information Security Manager), namenjenega upravljalcem in odločevalcem organizacij. V skladu s tem je tudi seminar razdeljen na štiri področja:
Vodenje informacijske varnosti: organizacijska kultura, strukture, vloge in odgovornosti, strategija informacijske varnosti, ogrodja in standardi upravljanja informacij, metode pregleda informacijske varnosti…
Upravljanje tveganj informacijske varnosti: ogrodja za obvladovanje/upravljanje tveganj, ocena, vrednotenje tveganj, odziv na informacijska tveganja, spremljanje, poročanje in sporočanje o tveganjih…
Program informacijske varnosti: razvoj programa informacijske varnosti in sredstva/viri, standardi in ogrodja IV, metrike programa, varnostne kontrole…
Upravljanje incidentov: upravljanje incidentov in načrti odzivanja nanje, obvladovanje incidentov, obveščanje, odpravljanje, obnova in pregled incidenta, vpliv na poslovanje in neprekinjeno delovanje, načrtovanje obnovitve po nesreči…

Izobraževanje je namenjeno posameznikom, ki bi se radi naučili ali nadgradili znanja o upravljanju informacijske varnosti. Posebej je primerno za tiste, ki delujejo ali bi želeli delati na delovnih mestih, ki usmerjajo informacijsko varnost v podjetjih (vodja informacijske varnosti, vodja informatike, CISO ipd.). Izobraževanje je tudi dobra začetna točka za tiste, ki razmišljajo o certificiranju CISM.

Želena predznanja:
Osnovno poznavanje konceptov informacijske varnosti

Po zaključku izobraževanja bo udeleženec sposoben:
- prepoznati standarde, ogrodja in zahteve za upravljanje informacijske varnosti
- razpravljati o prednostih in pomanjkljivostih skladnosti z varnostnimi zahtevami
- oblikovati strateški varnostni načrt in varnostno politiko
- razumeti običajna tveganja in kontrole na področju informacijske varnosti
- razumeti kompleksnost upravljanja ljudi, procesov in tehnologije za doseganje informacijske varnosti
- prepoznati osnovne ekonomske zahteve in zahteve po virih, ki so potrebni za doseganje ciljev organizacije na področju informacijske varnosti

EDIH DIGI-SI 2

Projekt EDIH DIGI-SI (European Digital Innovation Hub Slovenija) predstavlja nacionalno vozlišče za digitalno transformacijo MSP-je v Sloveniji, ki deluje v okviru evropske mreže EDIH pod okriljem programa Digitalna Evropa. Namen projekta je pospeševanje uvajanja naprednih digitalnih tehnologij, predvsem umetne inteligence, visokozmogljivega računalništva, **kibernetske varnosti**, podatkovnih tehnologij ter digitalizacije poslovnih procesov.

Konzorcij DIGI-SI povezuje univerze, raziskovalne institucije, tehnološke centre, razvojne agencije in gospodarske partnerje, ki skupaj zagotavljajo strokovno podporo malim in srednje velikim podjetjem ter organizacijam javnega sektorja pri prehodu v digitalno gospodarstvo.

Ključne aktivnosti projekta vključujejo svetovanje pri digitalni preobrazbi, testiranje tehnologij pred investicijo (“test before invest”), usposabljanja zaposlenih za razvoj digitalnih kompetenc, podporo pri dostopu do financiranja ter povezovanje podjetij z raziskovalnimi in inovacijskimi ekosistemi. Poseben poudarek je namenjen praktični uporabi umetne inteligence, podatkovne analitike, interneta stvari in avtomatizacije procesov za izboljšanje konkurenčnosti organizacij. DIGI-SI podjetjem omogoča dostop do strokovnjakov, laboratorijev in demonstracijskih okolij, kjer lahko preizkusijo nove digitalne rešitve brez visokih začetnih tveganj.

Projekt ima pomembno vlogo tudi pri zmanjševanju digitalnega razkoraka med regijami in sektorji, saj spodbuja vključevanje manjših podjetij ter organizacij, ki pogosto nimajo lastnih razvojnih kapacitet za uvajanje naprednih tehnologij. S povezovanjem slovenskega inovacijskega prostora z evropskimi partnerji EDIH DIGI-SI prispeva k večji tehnološki suverenosti, trajnostnemu razvoju in dolgoročni konkurenčnosti slovenskega gospodarstva v evropskem digitalnem prostoru.

O SRIP GoDigital

Strateško razvojno inovacijsko partnerstvo SRIP GoDigital predstavlja razvojni korak za krepitev IKT panoge in možnost boljše podpore ZIT članom na področju razvoja inovativnih digitalnih storitev in produktov. Njegovo poslanstvo je osredotočenje raziskovalnih in inovacijskih kapacitet ter vlaganj za razvoj in trženje zahtevnejših, celovitih in integriranih digitalnih storitev, izdelkov in rešitev v dialogu s člani in oblikovalci politik. Ena od ključnih aktivnosti je tudi krepitev naprednih kompetenc IKT strokovnjakov ter spodbujanje vseživljenjskega učenja, s ciljem ustrezno opremiti zaposlene v slovenskem gospodarstvu z novimi znanji in veščinami. S tem SRIP GoDigital prispeva k večji prilagodljivosti, inovativnosti in konkurenčnosti slovenskega IKT sektorja.

O Sekciji za kibernetsko varnost pri združenju za informatiko in telekomunikacije

V okviru Združenja za informatiko in telekomunikacije pri GZS deluje Sekcija za kibernetsko varnost (SeKV), ki se osredotoča na združevanje in usklajevanje interesov uporabnikov in ponudnikov kibernetskih varnostnih rešitev. Poslanstvo SeKV je z aktivnim sodelovanjem z vsemi deležniki kibernetske varnosti spodbuditi razvoj kibernetskih zmogljivosti slovenskih podjetij ponudnikov in uporabnikov storitev ter prispevati k celostnemu razvoju kibernetske varnosti v RS.

O CyberHub Slovenija

V okviru projekta CyberHub je bilo vzpostavljeno slovensko stičišče znanj in veščin za kibernetsko varnost (CyberHub Slovenija). Zasnovano je kot strateška platforma za povezovanje strokovnjakov s področja kibernetske varnosti, strokovnih združenj in pobud, ponudnikov rešitev in storitev na področju kibernetske varnosti, predstavnikov uporabnikov rešitev, institucij znanja ter oblikovalcev politik. V okviru projekta se je izvedla analiza stanja in potreb po strokovnjakih na področju kibernetske varnosti ter njihovih veščinah in kompetencah. Med drugim bomo na podlagi teh analiz v okviru stičišča oblikovali tudi projektno nacionalno strategijo za izboljšanje stanja kibernetske varnosti v Sloveniji ter organizirali različne aktivnosti za ozaveščanje.