Univerza v Mariboru
Fakulteta za elektrotehniko, računalništvo in informatiko
Koroška cesta 46
2000 Maribor, Slovenija

Celovit pregled in analiza izobraževanj na področju kibernetske varnosti

Projekt Ciljnega raziskovalnega programa CRP 2021 št. V2-2132 »RUKIV - Razvoj programov usposabljanj za kibernetsko varnost«

Poročilo delovnega paketa 1: PREGLED

Urednik: Muhamed Turkanović

Avtorji dokumenta: Marko Kompara, Lili Nemec Zlatolas, Marko Hölbl, Tatjana Welzer Družovec, Leon Bošnjak, Polona Vodopivec, Milan Gabor, Muhamed Turkanović

Maribor, januar 2022

Rezultati, pridobljeni znotraj tega projekta, so bili financirani s strani ARRS in URSIV pod pogodbo št. V2-2132.

Sodelujoče institucije v projektu RUKIV

KRATICA	NAZIV
UM FERI	Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko
VIRIS	Viris, varnost in razvoj informacijskih sistemov, d. o. o.

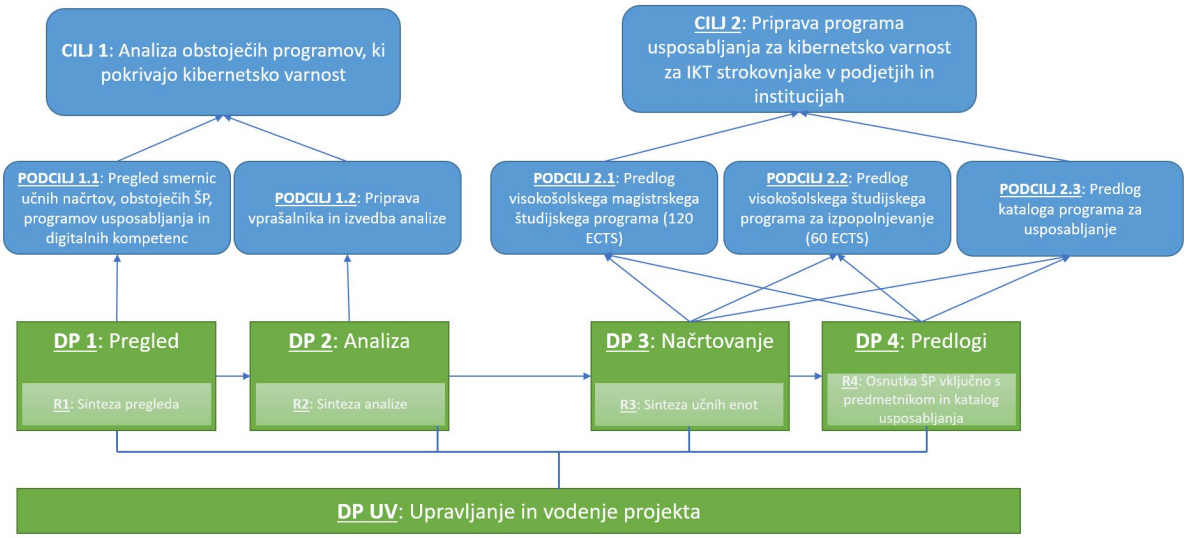
Zagotavljanje kakovosti dokumenta

Zagotavljanje kakovosti dokumenta	Katja Kerman, UM FERI Polona Vodopivec, VIRIS

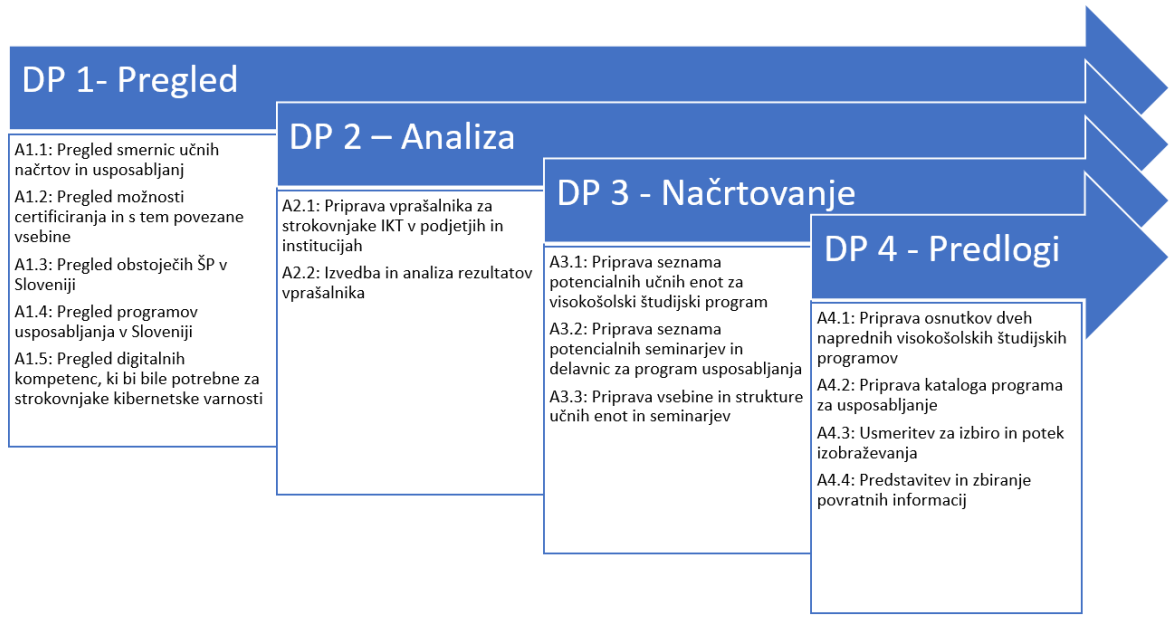
Kazalo

1 Uvod

Ob koncu DP1 načrtujemo zaključen in celovit rezultat v obliki sinteze posameznih podrobnejših analiz, izvedenih med aktivnostmi A1.1 – A1.5. Rezultati sinteze bodo zbrani v krajšem internem poročilu, ki bo služilo kot osnova za naslednje DP. Poročilo bo tako predstavilo celovito trenutno stanje na področju izobraževalnih programov na področju kibernetske varnosti na visokošolski ravni in programov usposabljanja, in sicer s fokusom na že obstoječe in delovno-aktivne IKT strokovnjake.



Slika 1: Delovni paketi, rezultati in podcilji.



Slika 2: Program dela vključno s posameznimi aktivnostmi po delovnih paketih.

2 Pregled smernic in priporočil izobraževanj in usposabljanj

Izobraževanje na področju kibernetske varnosti je razširjeno po celotnem svetu. Poznamo več vrst izobraževanj, pri čemer so določena neformalna in določena formalna. Med slednja štejemo tista izobraževanja, kjer si udeleženci ob koncu pridobijo uradno priznane diplome s strani akreditiranih višje ali visokošolskih ustanov in s tem povezano višjo stopnjo izobrazbe. Za tehnična visokošolska izobraževanja obstajajo priporočila in smernice s strani svetovno priznanih organizacij in združenj, kot so IEEE (Institute of Electrical and Electronics Engineers), ACM (Association for Computing Machinery) itn. Izvedli smo pregled teh smernic in smernic za splošna usposabljanja s strani organizacij, kot so ENISA (European Union Agency for Cybersecurity) in NIST (National Institute of Standards and Technology) ter pregled morebitnih drugih strokovnih del na to temo, pri čemer smo identificirali naslednje pomembne reference:

- Joint Task Force on Cybersecurity Education (ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8). 2018. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, New York, NY, USA.
- ENISA, Cybersecurity skills development in the eu - The certification of cybersecurity degrees and ENISA's Higher Education Database. 2019.
- The European Cyber Security Organisation (ESCO). WG5 PAPER European Cybersecurity Education and Professional Training: Minimum Reference Curriculum. 2021.

Poročilo s strani ENISA glede razvoja znanj s področja kibernetske varnosti podaja pregled stanja visokošolskega izobraževanja s področja KV v Evropski uniji, pri čemer podajajo tudi osnovo za analizo področja visokošolskih študijskih programov (ŠP), ki to področje naslavljajo. Poročilo je tudi osnova za platformo CYBERHEAD, ki predstavlja javno dostopno zbirko kvalificiranih ŠP v EU. Med drugim definirajo pogoje pod katerimi se lahko določen ŠP kvalificira kot ŠP s področja KV in sicer: (1) mora imeti določeno minimalno število ECTS, ki so neposredno namenjeni tematikam informacijske in kibernetske varnosti (tj., 25 % za 1. stopnjo, 40 % za 2. stopnjo), (2) mora imeti strukturiran kurikulum, ki po možnosti vključuje praktično komponento usposabljanja, (3) je del visoko kakovostne akreditirane visokošolske ustanove, ki lahko vključuje predavatelje iz industrije, (4) vključuje širši multi-/interdisciplinarni fokus, ter (5) ponuja dejavnost ozaveščanja in sodelovanja s preostalimi nacionalnimi službami za kibernetsko varnost.

Poročilo s strani ESCO se v uvodu sklicuje na smernice in ogrodja, ki so prav tako identificirani v tem poglavju in v kasnejšem pregledu smernic za kompetence (npr. CyBOK), pri čemer predstavlja tudi predloge izvedbe procesa snovanja visokošolskega kurikuluma za področje KV. Proces definira štiri faze, ki so skladne z načrtovanimi aktivnostmi tega projekta (pridobivanje informacij, predstavitev dejstev, priprava rezultatov in predlogov ter pridobivanje pogledov). Poročilo nadaljuje z vsebino predlogov grobe strukture kurikuluma ŠP KV, ki bi naj pokrivalo razen tehnologij, orodij in ogrodij za KV tudi upravljanje informacijske varnosti, vključujoč organizacijski in človeški vidik, hkrati pa tudi efektivna uporaba znanj s področja KV s fokusom na pridobivanje praktičnih znanj (cyber range, penetracijsko testiranje, CTF itn.) ter integracijo z naprednimi tehnologijami, kot so umetna inteligenca, navidezna resničnost, oblačne infrastrukture itn. Poročilo zaključi s predlogom referenčnega kurikuluma, ki sledi standardom priprave učnih enot in načrtov po Bloomovi taksonomiji vendar le to ni definirano kot zaključen študijski program 1. ali 2. stopnje.

Najobsežnejši rezultati smernic in priporočil za področje KV izhaja iz ACM&IEEE priporočil za kurikulum kibernetske varnosti. Poročilo gradi smernice za načrte kurikuluma na osnovi predhodnih rezultatov dela v izobraževanju, usposabljanju in razvoju delovne sile na področju kibernetske varnosti in med drugim uporablja vire kot npr. NICE Cybersecurity Workforce

Framework in zahteve Nacionalnih centrov akademske odličnosti za kibernetsko varnost. Vključuje štiri ključne komponente: (1) pregled discipline kibernetske varnosti za namen oblikovanja kurikularnega modela, (2) predstavitev kurikularnega okvirja in oris priporočenih vsebin, (3) pregled pogleda industrije na področje kibernetske varnosti ter (4) drugi podrobni predlogi za proces razvoja učnih načrtov in kurikuluma povezani z referencami, delovno silo, institucijami itn. Med drugim definira disciplino KV kot interdisciplinarno področje, ki zajema številne faktorje, kot so človeški, etični, zakonski, upravljavski vidiki, ki pa so tesno odvisne in povezane z tehničnimi disciplinami, kot so računalništvo in informatika, informacijske tehnologije, informacijski sistemi ter razvoj programske opreme. Priporočila so še posebej izčrpna iz vidika priporočene vsebine, ki je razdeljena na t. i. glavna področja znanj. Teh področij je osem, ki so posledično še podrobneje razdeljena na podenote itn. Le to smo izbrali tudi sami kot osnovno za nadaljnjo analizo, pri čemer je več o področjih znanj opisano v poglavju 6.2.

3 Pregled možnosti certificiranja in s tem povezane vsebine

Certifikat je potrdilo o znanju in veščinah posameznika. Organizacije, ki izvajajo certificiranje pogosto ponujajo tudi izobraževanja in usposabljanja, ki pripravijo kandidate na situacije, s katerimi se bo soočal v svojem profesionalnem življenju in neko obliko preizkušanja znanja, ki je tipično zadnji korak pred pridobitvijo certifikata.

Certifikati poleg znanja in veščin, ki jih kandidati pridobijo med pripravami na certificiranje, nudijo še druge dobre lastnosti. Osebe s certificiranim znanjem imajo boljše možnosti zaposlitve, medtem ko so lahko, na zahtevnejših delovnih mestih določeni certifikati celo zahtevani in ne predstavljajo več samo prednosti. Skozi postopek certificiranja, se kandidati pogosto spoznajo s predavatelji in drugimi sodelujočimi, ki želijo pridobiti certifikat ter se na takšen način mrežijo in širijo svoje kontakte in vpetost v strokovno skupnost. Poleg tega pridobljeni certifikati tudi pokažejo resnost oz. zanimanje za delo na področju certificiranja, izkaže profesionalno kredibilnost, so lahko vzvod za napredovanje v službi in služijo kot način nadgrajevanja prejšnjih znanj in zagotavlja skladnosti znanj in veščin z napredkom/spremembami, ki so se zgodile na področju, ki jih certifikat pokriva. Večino takšnih certifikatov je potrebno obnavljati vsakih nekaj let. Vse te lastnosti veljajo tudi za certificiranje na področju kibernetske varnosti.

V raziskavi[1], ki jo je opravil (ISC)^2 so ugotovili, da organizacije v Združenih državah Amerike v 70 % in globalno v 78 % primerih zahtevajo certificiranje od svojih zaposlenih strokovnjakov za kibernetsko varnost. V isti raziskavi so tudi ocenili, da imajo certificirani zaposleni na področju kibernetske varnosti v povprečju šestnajst tisoč evrov višjo letno plačo.

Najbolj znane organizacije za certificiranje s področja kibernetske varnosti so **CompTIA**, **EC-Council**, **eLearn Security**, **GIAC** (Global Information Assurance Certification), **ISACA** (Information Systems Audit and Control Association), **Offensive Security** in **(ISC)^2** (International Information System Security Certification Consortium). To seveda niso vsi ponudniki, ki obstajajo. Ti so samo bolje sprejeti (boljše so poznani in iskani v industriji) in ponujajo bolj celovit nabor certifikatov za področje kibernetske varnosti. Poleg takšnih ponudnikov, poznamo še ponudnike, ki izvajajo certificiranje za lastne storitve oz. opremo. Takšni certifikati in pridobljeno znanje je torej specifično za dano storitev ali opremo. Primeri takšnih organizacij oz. ponudnikov certifikatov so Google, Amazon, Microsoft in Cisco. Tudi takšne organizacije pogosto vključujejo certifikate, povezane s kibernetsko varnostjo.

Sekcija za Kibernetsko Varnost (SeKV) Gospodarske zbornice Slovenije (GZS) ima na spletni strani objavljen seznam certifikatov za kibernetsko varnost[2]. Seznam je razporejen glede na zahtevnost pridobitve certifikata in področja kibernetske varnosti. Seznam ni izčrpen, ampak vključuje dober pregled in skoraj vse od desetih najbolj iskanih certifikatov, glede na rezultate raziskave, ki jo je izvedla Coursera[3]. V raziskavi, opravljeni v prvi polovici 2021, so v objavljenih razpisih na platformah LinkedIn, Indeed in Simply Hired za nove zaposlitve v Združenih državah Amerike iskali, kateri certifikati se najpogosteje pojavijo v besedilih razpisov. Vseh 10 najpogosteje iskanih certifikatov so izdale prej omenjene organizacije.

Spodaj (Tabela 1) je seznam certifikatov iz te raziskave v vrstnem redu od najbolj iskanega proti manj iskanim. V tabeli so podane še nekatere osnovne informacije o certifikatih. Cene certifikatov so različne in odvisne od statusa (npr. če je oseba član združenja) in tega ali certifikat vključuje tudi izobraževanje. Cene začnejo pri nekaj sto evrov in lahko dosežejo nekaj tisoč evrov. V tabeli

[1] https://blog.isc2.org/isc2_blog/2021/01/cybersecurity-workforce-study-certifications-boost-salaries-by-an-average-of-18000.html
[2] https://www.gzs.si/sekv/Certifikati
[3] https://www.coursera.org/articles/popular-cybersecurity-certifications

smo vključili okvirno ceno, saj je ta pogosto odvisna od lokacije, možnih dogovorov med organizacijami, valute itd. Določeni izvajalci zahtevajo tudi članstvo, kjer članarine niso vštete v navedene zneske. Nekateri certifikati na tem seznamu imajo predpogoje, ki jih kandidati morajo izpolnjevati, preden lahko pridobijo certifikat. Tipično so ti predpogoji delovna doba na področjih kibernetske varnosti. Kljub temu večina certifikatov na seznamu nima predpogojev, vendar to ne pomeni, da so certifikati osnovni, saj še vedno priporočajo predznanje različnih področij, ki so osnova za znanja in veščine, zajete v certifikatu. Predpogoji so v veliki meri odvisni tudi od izvajalca.

Tabela 1: Seznam desetih najbolj zahtevanih certifikatov s področja kibernetske varnosti.

Naziv	Izvajalec	Cena	Zahtevnost	Veljavnost	Vsebina
CISSP	$(ISC)^2$	665€	Srednja	3 leta	Varnost in upravljanje tveganj, varovanje sredstev, varnostna arhitektura in inženiring, komunikacijska in omrežna varnost, upravljanje identitet in dostopa, ocenjevanje varnosti in testiranje, varnostno delovanje in varnost pri razvoju programske opreme.
CISA	ISACA	500 - 670€	Srednja	3 leta	Postopek revizije informacijskih sistemov, upravljanje in vodenje IT, razvoj in implementacija informacijskih sistemov, delovanje informacijskih sistemov in poslovna odpornost in zaščita informacijskih sredstev.
CISM	ISACA	500 - 670€	Srednja	3 leta	Upravljanje informacijske varnosti, upravljanje tveganj, razvoj in upravljanje programov informacijske varnosti in upravljanje incidentov.
Security+	CompTIA	334€	Nizka	3 leta	Grožnje, napadi in ranljivosti, upravljanje identitet in pravic dostopa, tehnologije in orodja, arhitektura in oblikovanje, kriptografija in infrastruktura javnih ključev (PKI).
CEH	EC-Council	840 - 1060€	Srednja	3 leta	Uvod v etično hekanje, iskanje sledi in izvidništvo, skeniranje omrežij, analiza ranljivosti, hekanje sistemov, zlonamerna programska oprema, sniffing, socialni inženiring, DoS, ugrabitev seje, izogibanje identifikatorjem, požarni pregradi in Honeypotom, hekanje spletnih strežnikov in spletnih aplikacij, SQL vrivanje, hekanje brezžičnih omrežij, hekanje mobilnih platform, hekanje IoT in OT,in kriptografija.
GSEC	GIAC	2200€	Nizka	4 leta	Nadzor dostopa in upravljanje gesel, kriptografija, kriptografski algoritmi in uporaba, preprečevanje izgube

Naziv	Izvajalec	Cena	Zahtevnost	Veljavnost	Vsebina
					podatkov in varnost mobilnih naprav, obrambna arhitektura omrežja, varnost končnih točk, obravnava incidentov in odzivanje nanje, zmanjševanje škodljive kode, omrežje in protokoli, varnostni okviri, skeniranje ranljivosti in penetracijsko testiranje, varnost brezžičnega omrežja.
SSCP	(ISC)²	230€	Nizka	3 leta	Nadzor dostopa, varnostne operacije in upravljanje, prepoznavanje, spremljanje in analiziranje tveganj, odzivanje na incidente in okrevanje, kriptografija, varnost omrežij in komunikacije ter varnost sistemov in aplikacij.
CASP+	CompTIA	419€	Srednja	3 leta	Upravljanje tveganj, upravljanje ranljivosti, organizacijska varnost, uporabljena kriptografija, integrirana varnost gostitelja, varen razvoj, arhitektura omrežne varnosti, varna konfiguracija. omrežja, skeniranje in spremljanje, upravljanje identitet, odzivanje na incidente.
GCIH	GIAC	2200€	Srednja	4 leta	Odzivanje na incidente in kibernetske preiskave, izvidništvo, skeniranje, napadi na gesla in dostop, napadi z javnim prikazovanjem in "drive-by" napadi, izogibanje napadom in napadi po uspešnem napadu.
OSCP	Offensive Security	880€+	Visoka	Ne zastara	Ukazi za Linux in Windows, Bash Scripting, pasivno in aktivno zbiranje informacij, skeniranje ranljivosti, napadi na spletne aplikacije, prekoračítev medpomnilnika, napadi na strani odjemalca, iskanje znanih ranljivosti, odpravljanje ranljivosti, izogibanje protivirusnim programom, povečevanje privilegijev, napadi na gesla, preusmerjanje vrat in tuneliranje, napadi na aktivni imenik in ogrodje Metasploit.

Tukaj je še nabor vseh certifikatov, ki jih ponuja sedem prej naštetih glavnih ponudnikov certifikatov na področju kibernetske varnosti, ki niso tudi ponudniki storitev oz. proizvajalci opreme.

CompTIA

- Advanced Security Practitioner (CASP+)
- Cybersecurity Analyst (CySA+)
- PenTest+
- Security+

EC-Council

- Advanced Network Defense (CAST 614)
- Certified Application Security Engineer (CASE)
- Certified Blockchain Professional (CBP)
- Certified Encryption Specialist (ECES)
- Certified Ethical Hacker (CEH)
- Certified Ethical Hacker (CEH) Master
- Certified Incident Handler (ECIH)
- Certified Network Defender (CND)
- Certified Network Defense Architect (CDNA)
- Certified Penetration Testing Professional (CPENT)
- Certified Secure Computer User (CSCU)
- Certified Security Specialist (ECSS)
- Certified SOC Analyst (CSA)
- Certified Threat Intelligence Analyst (CTIA)
- Computer Hacking Forensic Investigator (CHFI)
- Disaster Recovery Professional (EDRP)
- Licensed Penetration Tester (LPT) Master

eLearnSecurity

- eLearnSecurity Certified Digital Forensics Professional (eCDFP)
- eLearnSecurity Certified eXploit Developer (eCXD)
- eLearnSecurity Certified Incident Responder (eCIR)
- eLearnSecurity Certified Malware Analysis Professional (eCMAP)
- eLearnSecurity Certified Penetration Tester eXtreme (eCPTX)
- eLearnSecurity Certified Professional Penetration Tester (eCPPT)
- eLearnSecurity Certified Reverse Engineer (eCRE)
- eLearnSecurity Certified Threat Hunting Professional (eCTHPv2)
- eLearnSecurity Junior Penetration Tester (eJPT)
- eLearnSecurity Mobile Application Penetration Tester (eMAPT)
- eLearnSecurity Network Defense Professional (eNDP)
- eLearnSecurity Web Application Penetration Tester (eWPT)
- eLearnSecurity Web Application Penetration Tester eXtreme (eWAPTX)
- eLearnSecurity Web Defense Professional (eWDP)

GIAC

- Advanced Smartphone Forensics (GASF)
- Assessing and Auditing Wireless Networks (GAWN)
- Battlefield Forensics and Acquisition (GBFA)
- Certified Detection Analyst (GCDA)
- Certified Enterprise Defender (GCED)
- Certified Forensic Analyst (GCFA)
- Certified Forensic Examiner (GCFE)
- Certified Incident Handler (GCIH)
- Certified Intrusion Analyst (GCIA)
- Certified Project Manager (GCPM)
- Certified Web Application Defender (GWEB)
- Certified Windows Security Administrator (GCWN)
- Cloud Penetration Tester (GCPN)
- Cloud Security Automation (GCSA)
- Cloud Security Essentials (GCLD)
- Continuous Monitoring Certification (GMON)
- Critical Controls Certification (GCCC)
- Critical Infrastructure Protection (GCIP)
- Cyber Threat Intelligence (GCTI)
- Defending Advanced Threats (GDAT)
- Defensible Security Architecture (GDSA)
- Enterprise Vulnerability Assessor (GEVA)
- Exploit Researcher and Advanced Penetration Tester (GXPN)
- Foundational Cybersecurity Technologies (GFACT)
- Global Industrial Cyber Security Professional (GICSP)
- Information Security Fundamentals (GISF)
- Information Security Professional (GISP)
- Law of Data Security & Investigations (GLEG)
- Mobile Device Security Analyst (GMOB)
- Network Forensic Analyst (GNFA)
- Open Source Intelligence (GOSI)
- Penetration Tester (GPEN)
- Public Cloud Security (GPCS)
- Python Coder (GPYC)
- Response and Industrial Defense (GRID)
- Reverse Engineering Malware (GREM)
- Security Essentials (GSEC)
- Security Leadership (GSLC)

Security Operations Certified (GSOC)
Strategic Planning, Policy, and Leadership (GSTRT)
Systems and Network Auditor (GSNA)
Web Application Penetration Tester (GWAPT)

ISACA

Certified Data Privacy Solutions Engineer (CDPSE)
Certified in Risk and Information Systems Control (CRISC)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
Cybersecurity Practitioner Certification (CSX-P)

Offensive Security

Offensive Security Wireless Professional (OSWP)
Offensive Security Certified Expert 3 (OSCE3)
Offensive Security Certified Professional (OSCP)
Offensive Security Exploit Developer (OSED)
Offensive Security Exploitation Expert (OSEE)
Offensive Security macOS Researcher (OSMR)
Offensive Security Experienced Penetration Tester (OSEP)
Offensive Security Web Expert (OSWE)

(ISC)²

Certified Authorization Professional (CAP)
Certified Cloud Security Professional (CCSP)
Certified Information Systems Security Professional (CISSP)
Certified Secure Software Lifecycle Professional (CSSLP)
Systems Security Certified Practitioner (SSCP)

4 Pregled obstoječih študijskih programov v Sloveniji

Pregled študijskih smeri v Sloveniji je pokazal, da je na voljo en študijski program, ki se osredotoča na kibernetsko oz. informacijsko varnost. Visokošolski študijski program, ki se imenuje Informacijska varnost, obsega 3 leta študija in je ponujen s strani Fakultete za varnostne vede Univerze v Mariboru, po dokončanem izobraževanju pa študent/-ka prejme naziv diplomirani varstvoslovec/-ka informacijske varnosti. Študijski program zahteva pridobitev 180 ECTS oz. 27 uspešno opravljenih predmetov. Izmed 24 obveznih predmetov, se jih na kibernetsko varnost nanaša 5: Osnove informacijske varnosti (6 ECTS); Varnost informacijskih sistemov (6 ECTS); Zaščita podatkov in računalniška forenzika (6 ECTS); Varnost, zasebnost in zaupanje v mobilnih sistemih (5 ECTS); Varnost komunikacij, aplikacij in storitev (6 ECTS) in Kibernetska varnost (6 ECTS). Izmed 7 izbirnih predmetov se na kibernetsko varnost nanaša predmet Vedenjski vidiki informacijske varnosti (6 ECTS).

Nadaljnja analiza trenutnega stanja je razkrila, da večje število študijskih programov ponuja možnost izbire študijske smeri ali modula, ki se nanaša na kibernetsko varnost. Smeri ali module, ki se nanašajo na kibernetsko varnost, ponujajo štirje visokošolski zavodi, od tega trije javni in eden zasebni (Priloga A). Nadalje so trije moduli, ponujeni na drugi bolonjski stopnji ter ena študijska smer na prvi bolonjski stopnji. Fakulteta za elektrotehniko, računalništvo in informatiko Univerze v Mariboru ponuja študijsko smer Informacijska varnost na dodiplomskem univerzitetnem programu Informatika in tehnologije komuniciranja (sedaj Informatika in podatkovne tehnologije) ter modul Varnost IS in upravljanje z varnostjo na istoimenskem magistrskem študijskem programu. Fakulteta za računalništvo in informatiko Univerze v Ljubljani ponuja modul Omrežja in varnost na magistrskem študiju Računalništvo in informatika in ne nazadnje, Alma Mater ponuja modul Kibernetska varnost v sklopu magistrskega študija Spletna znanost in tehnologije.

Ne nazadnje se v sklopu 35 študijskih programov pojavljajo posamezni predmeti, ki se nanašajo na osnove kibernetske varnosti (Priloga B). Od 35 predmetov je eden ponujen na višješolskem študiju, 9 na visokošolskem študiju, 4 na prvi univerzitetni bolonjski stopnji, 17 na drugi bolonjski stopnji in 4 na doktorskem študiju. Skupno je 16 obveznih posameznih predmetov in 19 izbirnih.

Pregled študijskih smeri v povezavi s kibernetsko varnostjo v Evropskem prostoru razkrije, da se tovrstni študijski programi pretežno izvajajo na drugi bolonjski stopnji, natančneje je na voljo 134 magistrskih programov in 8 dodiplomskih programov. Magistrski študijski programi v Evropskem prostoru zajemajo 60 - 180 ECTS, najpogosteje 120 ECTS. Podroben pregled študijskih programov in njihov opis je pripravljen s strani ENISA-a[4], tj. CYBERHEAD.

[4] https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead

Tabela 2: Seznam študijskih programov, modulov in predmetov na slovenskih visokošolskih zavodih.

Študijski programi	**Število**
Fakulteta za varnostne vede UM	1
Moduli	**Število**
Fakulteta za elektrotehniko, računalništvo in informatiko UM	2
Fakulteta za računalništvo in informatiko UL	1
Alma Mater	1
Posamezni predmeti	**Število**
Mednarodna podiplomska šola Jožefa Stefana	5
Fakulteta za elektrotehniko, računalništvo in informatiko UM	5
Fakulteta za Komercialne in Poslovne Vede	4
Fakulteta za organizacijske vede UM	4
Fakulteta za računalništvo in informatiko UL	3
Fakulteta za elektrotehniko UL	2
Fakulteta za ekonomijo in informatiko	2
Alma Mater	2
Fakulteta za informacijske študije UNM	2
Gea College	2
B2	1
Fakulteta za Medije	1
Fakulteta za management in pravo	1
Poslovno-tehniška fakulteta	1

5 Pregled programov usposabljanja v Sloveniji

V Sloveniji kakor v tujini obstajajo številne organizacije, ki ponujajo različna usposabljanja, med katerimi so tudi tista tehnične narave. Določena usposabljanja so organizirana v obliki seminarjev ali delavnic, ki lahko trajajo po eno ali več ur, oziroma včasih tudi več dni. V sklopu A1.4 smo pregledali ponudbo usposabljanj v Sloveniji in identificirali tista, ki trenutno ponujajo kakršno koli vrsto usposabljanj na temo kibernetske varnosti ter ta klasificirati glede na ponudnika, vsebino, dolžino in tip.

Pregledali smo ponudbo vseh ponudnikov v Sloveniji, ki nudijo usposabljanja za kibernetsko varnost. Ponudnike smo iskali preko:

- kataloga strokovnjakov na spletni strani Digitalnega inovacijskega stičišča Slovenije (DIH),
- slovenskih fakultet, ki bi ponujale kakšno usposabljanje v zvezi s kibernetsko varnostjo,
- splošnega iskanja preko iskalnika na spletu.

Našli smo 18 različnih ponudnikov, ki ponujajo 27 različnih usposabljanj. Med temi ponudniki so v glavnem gospodarske družbe, nekaj pa je organizacij (inštituti, SI-CERT, ministrstvo, fakulteta itn.). Ob tem pa obstajajo tudi usposabljanja, ki so organizirana kot spremljevalna dejavnost konferenc in se vršijo v obliki delavnic. V glavnem se podjetja, ki ponujajo usposabljanja, primarno ukvarjajo z informacijsko varnostjo ali povezanimi IT-tehnologijami. Glavna tema vseh usposabljanj je področje etičnega hekanja in preverjanja varnosti sistemov. Večina ponudnikov ima podrobne opise usposabljanj z dolžino trajanja.

Kar se tiče cene, pa imajo nekateri zapisano tudi ceno, pri mnogih ponudnikih pa je cena po dogovoru (odvisna od števila udeležencev, trajanja itn.). Vseeno pa smo našli kar nekaj ponudnikov, ki o svojih usposabljanjih ponujajo malo podatkov. Nimajo podatkov o dolžini in ceni, kar 6 usposabljanj pa nima niti opisa vsebine.

Glede na tip usposabljanj kar nekaj podjetij ponuja on-line usposabljanja – od »on-line treninga«, »on-line usposabljanja«, »on-line tečaja« do »digitalnega tečaja«, »e-usposabljanja«, «interaktivnega tečaja« in »e-tečaja". Teh je devet. Našli smo pa tudi šest različnih tečajev, tri delavnice in prilagojeno usposabljanje.

Področja, ki so pokrita pri zbranih in analiziranih usposabljanjih, so:
- varnost programske opreme (ang. Software Security),
- varnost sistemov (ang. System Security),
- varnost ljudi (ang. Human Security),
- organizacijska varnost (ang. Organizational Security).

Področja, ki niso pokrita pri zbranih in analiziranih usposabljanjih, so:
- varnost podatkov (ang. Data Security),
- varnost komponent (ang. Component Security),
- varnost povezave (ang. Connection Security),
- družbena varnost (ang. Societal Security).

Tabela 3: Opis programov usposabljanj v Sloveniji.

1	**Tip in naslov usposabljanja:**	**tečaj - Varnost ICS/OT/IoT okolij**
	Ponudnik (ime in URL):	**SMART COM d. o. o.** www.smart-com.si/tecaj-varnost-ics-ot-iot-okolij/
	Vsebina:	V tem **4-dnevnem tečaju** boste preko predavanj in praktičnih vaj prilagojenih vašemu sektorju pridobili napredno poznavanje delovanja naprav, ki se nahajajo v industrijskih oz. procesnih okoljih (ICS/OT/IoT) in okoljih kritične infrastrukture, s poudarkom na razumevanju kibernetske varnosti v teh okoljih, poznavanju varnostnih ranljivosti in kako učinkovito zaščititi okolje pred zlorabami in hekerskimi napadi za zagotavljanje neprekinjenega delovanja. Tečaj je sestavljen iz naslednjih vsebinskih sklopov, razdeljenih v 4 dneve. **1 DAN** Seznanili se boste z osnovno strukturo, protokoli in kibernetsko obrambo komunikacij v industrijskih oz. procesnih okoljih in v kritični infrastrukturi (ICS/OT/IoT). Spoznali boste protokole, ki se uporabljajo v teh okoljih (Modbus, Profinet, S7…) ter možne načine izrabe njihovih ranljivosti oz. pomanjkljivosti, ki jih napadalci lahko izkoristijo. V obliki laboratorijskih vaj se boste preizkusili v realnih primerih in postopkih napada ter spoznali rešitve, s katerimi takšen napad preprečite. **2 DAN** Seznanili se boste s *Purdue Enterprise Reference Architecture* (PERA) 6-nivojskim referenčni modelom IT in OT okolja, kjer se boste posvetili napravam in tehnologijam iz štirih področij (Nivo 0 – Nivo 3) ter načinom, kako se te naprave in tehnologije povezujejo in zlorabljajo s strani napadalcev. Spoznali boste segmentacijo omrežja v ICS/OT/IoT okoljih ter ravni/sloje in varnostne okvirje omrežja. Seznanili in primerjali boste distribuirane sisteme (DCS) s sistemi SCADA ter ostalimi elementi operativne tehnologije (OT) ter si ogledali njihove pomanjkljivosti in ranljivosti. **3 DAN** Spoznali se boste s tehnikami in metodologijami, ki jih napadalci uporabljajo za vdor v industrijska oz. procesna okolja in v kritično infrastrukturo (ICS/OT/IoT okolja). V obliki laboratorijske vaje se boste sami preizkusili v vlogi napadalca, kot tudi tistega, ki mora zagotavljati ustrezno kibernetsko varnost v teh okoljih. Pri tem boste uporabljali najsodobnejša orodja z vgrajenimi mehanizmi strojnega učenja in umetne inteligence ter spoznali, kako z njihovo uporabo preprečite nadaljnje aktivnosti napadalcev. **4 DAN** Povzeli boste korake najboljše prakse pri gradnji varnosti oz. oblikovanju varnostnih politik za industrijska oz. procesna okolja in kritično infrastrukturo (ICS/OT/IoT okolja). Seznanili se boste z vsemi potrebnimi elementi, ki jih je potrebno upoštevati za zagotavljanje kibernetskega varovanja v sistemih operativne tehnologije (OT). V obliki laboratorijske vaje boste postavili celoten

		sistem OT z osnovnimi elementi varovanja ter s tem prikazali razumevanje podane tematike. ***5. DAN (opcijsko)*** Skozi praktično delavnico boste vzpostavili manjše IoT okolje, kjer boste vzpostavili svoj sistem za nadzor in upravljanje senzorjev ter krmiljenje naprav, pri tem pa upoštevali elemente kibernetske varnosti. Po zaključku delavnice boste končan izdelek lahko odnesli s seboj in ga uporabili v lastne namene.
	Dolžina:	4 dni
	Cena:	1.500 € + DDV (dodatni dan, tj. 5. dan znaša še dodatnih 300 €+ DDV)
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
2	**Tip in naslov usposabljanja:**	**spletni seminar – 30 minut za informacijsko varnost na delovnem mestu**
	Ponudnik (ime in URL):	**SI-CERT** www.varninainternetu.si/za-kibernetsko-varnost-lahko-najvec-naredimo-uporabniki-sami/
	Vsebina:	Ogromno spletnih prevar se prične zgolj z enim napačnim klikom, ki pa ima lahko za uporabnika strašanske posledice. Večina prevar je posledica človeške napake, zato bi mnoge izmed njih lahko uspešno preprečili, če bi si pred vsakim klikom vzeli sekundo za premislek. »Premisli, preden klikneš« je tudi letos slogan evropskega meseca kibervarnosti, ki državljane in državljanke EU ozavešča o spletni varnosti. Slovenija bo tudi letos sodelovala pri aktivnostih s programom ozaveščanja Varni na internetu, ki ga koordinira Nacionalni odzivni center za kibernetsko varnost SI-CERT. V sklopu letošnje kampanje smo na SI-CERT zasnovali brezplačni spletni tečaj o informacijski varnosti za zaposlene Varni v pisarni, do katerega lahko uporabniki že dostopate na portalu.
	Dolžina:	30 minut
	Cena:	brezplačno
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
3	**Tip in naslov usposabljanja:**	**on-line trening – Informacijska varnost za zaposlene**
	Ponudnik (ime in URL):	**B2 d. o. o.** www.b2.eu/cyber www.b2.eu/sl/e-izobrazevanje/e-gradiva/informacijska-varnost-za-zaposlene
	Vsebina:	Program osveščanja za zaposlene E-izobraževanje je zasnovano na praktičnih primerih kibernetskih nevarnosti in podkrepljeno z najnovejšimi primeri zlorab iz prakse. Sestavljajo ga: • kratki moduli on-line izobraževanja, • praktični primeri, iz katerih se zaposleni naučijo pravilno reagirati, • praktične učne igre, • primeri iz dejanskih slovenskih praks (socialni inženiring, e-poštni napadi, phishing), • pomoč in recepti za ukrepanje v primeru zlorab.
	Dolžina:	Ni podatka
	Cena:	Ni podatka, potrebno poslati povpraševanje

		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
4	**Tip in naslov usposabljanja:**	**ni podatka o tipu – Osnovni vidiki kibernetske varnosti**
	Ponudnik (ime in URL):	**Institut ICS Ljubljana** www.ics-institut.si/center-informacijske-varnosti
	Vsebina:	Vsebina izobraževanja: • vrednost informacij in vrste informacij • načini uporabe informacij • koncepti kibernetske varnosti • informacijska in računalniška varnost • ranljivosti in grožnje • upravljanje kibernetske varnosti • vzpostavitev ustreznih procesov za zagotavljanje kibernetske varnosti • vloga kadrovskega potenciala na področju kibernetske varnosti
	Dolžina:	Ni podatka
	Cena:	Ni podatka, potrebno jih je kontaktirati za ponudbo
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
5	**Tip in naslov usposabljanja:**	**ni podatka o tipu – Tveganja socialnega Inženiringa pri zagotavljanju kibernetske varnosti podjetja**
	Ponudnik (ime in URL):	**Institut ICS Ljubljana** www.ics-institut.si/assets/uploads/files/Program-strokovnih-izobraževanj-instituta-ICS-Ljubljana.pdf
	Vsebina:	Ni podatka
	Dolžina:	Ni podatka
	Cena:	Dogovorjeno z naročnikom glede na število udeležencev
		Podatki, pridobljeni januar 2022
6	**Tip in naslov usposabljanja:**	**ni podatka o tipu – Osnovni vidiki kibernetske varnosti v podjetju**
	Ponudnik (ime in URL):	**Institut ICS Ljubljana** www.ics-institut.si/assets/uploads/files/Program-strokovnih-izobraževanj-instituta-ICS-Ljubljana.pdf
	Vsebina:	Ni podatka
	Dolžina:	Ni podatka
	Cena:	Dogovorjeno z naročnikom glede na število udeležencev
		Podatki, pridobljeni januarja 2022
7	**Tip in naslov usposabljanja:**	**on-line izobraževanje – Informacijska varnost pri delu od doma**
	Ponudnik (ime in URL):	**Založba Forum Media, založniška dejavnost d. o. o** www.zfm.si/izdelek/informacijska-varnost-pri-delu-od-doma/
	Vsebina:	Predavanje: Zagotavljanje IT varnosti pri delu od doma Predavanje: Notranji varnostni incidenti in tveganja povezana z delom od doma

	Dolžina:	Ni podatka, spletna učilnica je odprta 2 meseca
	Cena:	Ni podatka, potrebno jih je kontaktirati za ponudbo
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
8	**Tip in naslov usposabljanja:**	**tečaj – Ethical Hacking**
	Ponudnik (ime in URL):	**Housing** www.housing.si/Tecaji/Ethical_Hacking_1
	Vsebina:	Petdnevni tečaj etičnega hekanja zajema: • OSINT metodologije – vsak tečajnik bo na primeru svojega podjetja pasivno preiskal javno dostopne podatke, IP naslovni prostor, poddomene, metapodatke, indeksirane spletne strani idr. Spoznali bomo spletne storitve, ki nenehno zbirajo informacije o spletu. Velikokrat se pokažejo informacije, za katere si podjetja ne želijo, da so javno dostopne. • Pregled zunanjega omrežja – pregledali bomo aktualne spletne napade in na podlagi predpripravljenega laboratorija spoznali, kako napadalci vdirajo in izrabijo infrastrukturo podjetij iz zunanjega omrežja. Podrobneje si bomo ogledali napade na ključne strežnike (dns, smtp, ipd.) ter prikazali, kako lahko iz zunanjega omrežja vdremo v infrastrukturo notranjega omrežja organizacije. Udeleženci skozi vodene primere aktivno spoznavajo hekerska orodja in metodologije. Poseben poudarek posvetimo tudi dnevniškim datotekam in odkrivanju napadov. • Pregled spletnih strani – udeleženci tečaja se seznanijo z OWASP TOP 10 metodologijo ter najpogostejšimi vdori na spletnih straneh. V predpripravljenem laboratoriju je več ranljivih spletnih strani na različnih mestih in različnih vratih, ki jih bodo morali tečajniki preko namigov sami odkriti. Nekatere ranljivosti so trivialne, druge zahtevajo več zaporednih korakov za popoln prevzem sistema. Na vodenih primerih spoznavamo najpogostejša orodja za vdore v spletne strani, posebej se osredotočamo na tiste primere, ki jih Špehonja z ekipo najpogosteje srečuje med izvedbo varnostnih pregledov ter penetracijskih testov v slovenskem okolju. • Pregled notranjega omrežja – pri izvedi notranjega varnostnega pregleda v 90 % organizacij že v prvem dnevu pridobimo vsaj en domenski uporabniški račun, ki odpira nove možnosti lateralnega gibanja po omrežju. Spoznali bomo, kako napadalci enumerirajo dosegljive naprave ter storitve, najpogostejše ranljivosti notranjega omrežja in jih na predpripravljeni domenski infrastrukturi tudi izkoristili. Spoznali se bomo tudi z drugimi tehnikami, kot so obratni inženiring ter binarna zloraba storitev.
	Dolžina:	5 dni
	Cena:	2.250 € + DDV
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
9	**Tip in naslov usposabljanja:**	**on-line tečaj – 2-dnevni online tečaj etičnega hekanja**
	Ponudnik (ime in URL):	**Housing**

		www.housing.si/Tecaji/2-dnevni_online_tecaj_eticnega_hekanja
	Vsebina:	Dvodnevni tečaj etičnega hekanja zajema: • OSINT metodologije – vsak tečajnik bo na primeru svojega podjetja pasivno preiskal javno dostopne podatke. IP naslovni prostor, poddomene, metapodatke, indeksirane spletne strani idr. Spoznali bomo spetne storitve, ki nenehno zbirajo informacije o spletu. Velikokrat se pokažejo infomacije, za katere si podjetja ne želijo, da so javno dostopne. • Pregled zunanjega omrežja – Pregledali bomo aktualne spletne napade in spoznali, kako napadalci vdirajo in izrabijo infrastrukturo podjetij iz zunanjega omrežja. Podrobneje si bomo ogledali napade na ključne strežnike (dns, smtp, web...). • Udeleženci skozi vodene primere aktivno spoznavajo hekerska orodja in metodologije. Poseben poudarek posvetimo tudi dnevniškim datotekam in odkrivanju napadov. Udeleženci lahko pod določenimi pogoji skenirajo tudi omrežje svoje organizacije. • Pregled notranjega omrežja – Pri izvedi notranjega varnostnega pregleda v 90 % organizacij že v prvem dnevu pridobimo vsaj en domenski uporabniški račun, ki odpira nove možnosti lateralnega gibanja po omrežju. Spoznali bomo, kako napadalci enumerirajo dosegljive naprave ter storitve, najpogostejše ranljivosti notranjega omrežja. Dotaknili se bomo tudi virusov, črvov, trojanskih konjev ter osnovnih tehnik obratnega inženiringa zlonamerne kode. V tem poglavju bodo udeleženci preverjali lastno (domače) notranje omrežje.
	Dolžina:	2 dni
	Cena:	740 € + DDV
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
10	**Tip in naslov usposabljanja:**	**tečaj – Etični heker**
	Ponudnik (ime in URL):	**Telekom Slovenije** www.telekom.si/poslovni-uporabniki/ponudba/resitve-za-podjetja/izobrazevalni-center/eticni-heking
	Vsebina:	Delavnica bo ponudila vpogled v naslednje teme: • Kako razmišljajo hekerji in katere metode uporabljajo • Podrobnejše poznavanje različnih hekerskih orodij in tehnik • Odkrivanje in izkoriščanje ranljivosti • Praktično preizkušanje posameznih metod in orodij
	Dolžina:	3 dni
	Cena:	1.899 € + DDV
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
11	**Tip in naslov usposabljanja:**	**on-line tečaj – Informacijska varnost**
	Ponudnik (ime in URL):	**Telekom Slovenije** www.telekom.si/poslovni-uporabniki/ponudba/resitve-za-podjetja/izobrazevalni-center/digitalni-tecaj-informacijska-varnost

	Vsebina:	Za ozaveščenost vseh končnih uporabnikov smo v okviru Varnostne akademije Izobraževalnega centra Telekoma Slovenije in v sodelovanju z svojimi partnerji pripravili digitalni tečaj »Informacijska varnost«, kjer se boste naučili osnove varne uporabe računalnika in računalniških omrežij.
	Dolžina:	Tečaj je v digitalni obliki, ki je za uporabnika časovno neomejen znotraj obdobja 6 mesecev.
	Cena:	Paket do 9 uporabnikov600,00 + DDV Paket 10 do 49 uporabnikov 1.400,00 + DDV Paket 50 do 149 uporabnikov 2.000,00 + DDV Paket 150 do 249 uporabnikov 2.900,00 + DDV Paket 250 do 499 uporabnikov 4.200,00 + DDV Paket 500 do 749 uporabnikov 5.900,00 + DDV
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
12	**Tip in naslov usposabljanja:**	**e-usposabljanje – Informacijska varnost**
	Ponudnik (ime in URL):	**MJU – Upravna akademija** www.ua.gov.si/aktivnosti/detajli/?ID=ac505edf-e669-ea11-9c51-005056818ee6&Tag=459
	Vsebina:	E-usposabljanje je namenjeno vsem državnim uslužbencem, ki želijo osvežiti znanje s področja informacijske varnosti. Vsebina: • informacijska varnost • najpomembnejši predpisi, ki urejajo področje informacijske varnosti • politika, postopki in prakse informacijske varnosti v državni upravi • osebna odgovornost varovanja informacij • grožnje informacijam in informacijskim sistemom • najboljše prakse zaščite informacijskih sredstev in podatkov tako v kot izven pisarne • odziv na sum incidenta ali na potrjen incident informacijske varnosti
	Dolžina:	2 pedagoški uri
	Cena:	Brezplačno
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
13	**Tip in naslov usposabljanja:**	**v učilnici, e-tečaj ali spletni seminar – prilagodijo se podjetju**
	Ponudnik (ime in URL):	**ASTEC** www.astec.si/default.asp?mid=sl&pid=izobraevanjeincertificiranje
	Vsebina:	Različna izobraževanja izvajamo v sklopu specifičnih licenčnih portfeljev.
	Dolžina:	Ni podatka
	Cena:	Ni podatka
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022

14	**Tip in naslov usposabljanja:**	**e-seminar (v spletni učilnici v živo) – Socialni inženiring: Kako ga prepoznati in preprečiti nepooblaščen dostop do našega informacijskega sistema?**
	Ponudnik (ime in URL):	**SIQ** www.siq.si/izobrazevanje/program/izobrazevanje/?e-seminar-socialni-inzeniring-kako-ga-prepoznati-in-prepreciti-nepooblascen-dostop-do-nasega-informacijskega-sistema&id=708DB3AE-3BDE-EB11-80FE-005056B80B8C
	Vsebina:	Udeležence želimo seznaniti s socialnim inženiringom ter različnimi vrstami napadov in tehnik socialnega inženiringa. Cilj je, da udeleženci po končanem izobraževanju znajo prepoznati socialni inženiring na podlagi znanja, ki ga osvojijo s pomočjo analiz praktičnih primerov. Na seminarju se boste seznanili z najnovejšimi tehnikami socialnega inženiringa z uporabo: • elektronskih sporočil, • spletnih strani, • prenosnih medijev, • telefona, • družabnih omrežij in • drugih tehnik.
	Dolžina:	Ni podatka
	Cena:	95 € + DDV
		Podatki, pridobljeni sept/okt 2021, *osveženi januar 2022*
15	**Tip in naslov usposabljanja:**	**interaktivni tečaj – Informacijska varnost in etično hekanje**
	Ponudnik (ime in URL):	**UNISTAR** www.proakademija.si/default.asp?mid=sl&pid=modul_it&wid=14119&detailid=89367
	Vsebina:	Vsebina tečaja: • Vrste neželene programske opreme (virusi, trojanski konji, rootkiti, črvi) • Statično raziskovanje neželene programske opreme (Detekcija zlonamerne kode) • Dinamično raziskovanje neželene programske opreme • Prikaz tehnik raznih napadov • Iskanje »zlonamernih« naprav v omrežju • Odkrivanje odprtih vrat in servisov na napravah • Odkrivanje ranljivih storitev v omrežju • Varnostni pregled spletnih strani • Vdori na spletne strani • Osnove OSINT-a • Google hacking
	Dolžina:	3 dni
	Cena:	Ni podatka
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
16	**Tip in naslov usposabljanja:**	**tečaj – Etični heking**

	Ponudnik (ime in URL):	**SNT Slovenija** www.snt.si/courses/eticni-heking/
	Vsebina:	Tečaj pokriva naslednje domene, ki so tudi predmet CEH tečaja, če se hoče kdo potem tudi certificirati: • Uvod v etično hekanje • Izvidnica • Skeniranje omrežij • Enumeracija sistemov in storitev • Sistemsko hekanje • Trojanci, virusi in črvi • Vohljači in različne male napravice • Socialno inženirstvo • DOS, DDOS, • Hekanje spletnih strežnikov in aplikacij • SQLi • Brezžična omrežja • Izogibanje detekcij • Kriptografija • Mobilne aplikacije • Penetracijsko testiranje
	Dolžina:	5 dni
	Cena:	1.950 €
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
17	**Tip in naslov usposabljanja:**	**ni podatka – piše le, da nudijo izobraževanja iz področja informacijske varnosti**
	Ponudnik (ime in URL):	**INFOCENTER** www.infocenter.si/izobrazevanje-in-usposabljanje/
	Vsebina:	Ni podatka
	Dolžina:	Ni podatka
	Cena:	Ni podatka
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
18	**Tip in naslov usposabljanja:**	**delavnice ob dogodkih**
	Ponudnik (ime in URL):	**Palsit** www.palsit.com
	Vsebina:	Izvajajo delavnice ob dogodkih
	Dolžina:	Ni podatka
	Cena:	Ni podatka
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
19	**Tip in naslov usposabljanja:**	**vnaprej pripravljeni e-tečaji – Informacijska varnost**
	Ponudnik (ime in URL):	**Smart Naris d. o. o.** www.esmartarena.com/e-izobrazevanje/
	Vsebina:	• **Delo od doma - Informacijska varnost** Tečajniki boste spoznali, zakaj je informacijska varnost pomembna, še posebej ko delamo od doma, katerim varnostnim tveganjem so izpostavljeni, katere tehnike hekerji najpogosteje uporabljajo pri izvajanju napadov na zaposlene, ki delajo od doma, kako prepoznati

		ali smo tarča napada ter kako se zaščititi, da ne postanemo žrtev hekerskega napada. • **Informacijska varnost** Tečaj je namenjen fizičnim osebam ter zaposlenim v podjetjih. Namen je preprečiti vdore in kraje podatkov iz računalnika in omrežij ter s tem preprečiti poslovno škodo in zlorabo osebnih podatkov. • **Informacijska varnost - Mobilne naprave** V tečaju boste spoznali, katere so najbolj ranljive točke vaše mobilne naprave, kako jih nepridipravi izkoriščajo in kaj lahko sami storite, da svoje mobilne naprave zavarujete pred napadalci. • **Informacijska varnost – Gesla** Ni podatkov • **Informacijska varnost - Socialni inženiring** V tečaju boste spoznali delovanje najpogostejše tehnike socialnega inženiringa, se naučili, kako jih prepoznati in kako se pred njimi ubraniti. • **Informacijska varnost - Varovanje podatkov** Varovanje podatkov v današnjem svetu postaja vedno bolj pomembno in kompleksno področje. V tečaju vam bomo predstavili različne nivoje zaščite podatkov, pokazali vam bomo kakšne metode tatovi informacij uporabljajo in kako dostop do svojih podatkov zavarovati pred nepooblaščenimi osebami. • **Osnove informacijske varnosti - E-pošta** - Izboljšati poznavanje informacijskih nevarnosti pri uporabi e-pošte - Znati prepoznati pasti - Poznati ukrepe pri okužbi z virusi in vdorih • **Informacijska varnost - Virusi & škodljiva programska oprema** V tečaju boste spoznali delovanje najbolj razširjenih oblik škodljive programske opreme in se naučili pravilno ravnati ob okužbi svojega računalnika. • **Informacijska varnost – Nevarnosti spleta** V tečaju boste spoznali glavne nevarnosti, ki na vas prežijo na spletu ter se naučili, kako jih prepoznati in se jim izogniti.
	Dolžina:	Različno – od 10 minut do 2 uri
	Cena:	10 minut – 15 € 15 minut – 24 € 20 minut – 15 € 25 minut – 15 € 2 uri – 63 €
		Podatki, pridobljeni sept/okt 2021, osveženi januar 2022
20	**Tip in naslov usposabljanja:**	**tečaj – Tečaj etičnega hekinga**
	Ponudnik (ime in URL):	**Viris d. o. o.** www.viris.si/storitve/tecaj-eticnega-hekinga/
	Vsebina:	Ponujamo različne tečaje, prilagojene različnim ciljnim skupinam. Tečaj etičnega hekanja ima širok razpon, in sicer od osnovnega do naprednega usposabljanja. Naš tečaj pokriva različna področja in prinaša izzive na naslednjih področjih: - O etičnem hekanju

		- OSINT in druga zbiranja informacij - Skeniranje in enumeracija - Izkoriščanje - Spletne aplikacije - Razbijanje gesel - Vzvratno inženirstvo - Hekanje oblačne infrastrukture Glede na veliko povpraševanje po SOC analistih ponujamo posebno izobraževanje, ki vam lahko pomaga, da zelo hitro začnete z izvajanjem SOC operacij. Tečaj pokriva naslednja področja: - OSINT in potencialne grožnje - Analiza dnevniških zapisov - Skeniranje za ranljivostmi - Nadzor omrežja - Wireshark - Kriptografija - Aplikacije in mobilna varnost - Omrežna varnost Za večje ekipe ali organizacije pripravimo posebej prirejene tečaje vašim sistemom, tehnologijam in platformam. S temi posebej prilagojenimi tečaji pridobite še več globine na področjih, ki so pomembni za vašo organizacijo.
	Dolžina:	1-5 dnevni tečaji
	Cena:	Po dogovoru
		Podatki, pridobljeni januarja 2022
21	**Tip in naslov usposabljanja:**	**tečaj – Tečaj varnega razvoja programske opreme**
	Ponudnik (ime in URL):	**Viris d. o. o.** www.viris.si/storitve/tecaj-varnega-razvoja-programske-opreme/
	Vsebina:	Ponujamo posebej prilagojene tečaje na področju varnega razvoja programske opreme v trajanju od 2 do 4 dni. Ker se zavedamo, da vsaka razvojna ekipa ali skupina razvijalcev potrebuje različne pristope, bomo za vsako skupino pripravili posebej prilagojen tečaj. Na našem tečaju se bodo udeleženci seznanili z: - trenutnim stanjem informacijske varnosti, - splošnimi vektorji napadov, - vektorji napada, ki so povezani s tehnologijo ali platformo, ki jo uporabljate, - OWASP TOP 10, - varnim razvojem programske opreme, - orodji, tehnikami in metodami testiranja programske opreme, - reševanjem nalog tipa CTF in tekmovali s soudeleženci. Naše tečajno okolje je prilagojeno vsakemu tečaju posebej in omogoča takojšnji začetek izvajanja tečaja brez nepotrebne priprave okolja in nameščanja različnih orodij.
	Dolžina:	2 do 4-dnevni tečaji
	Cena:	Po dogovoru
		Podatki, pridobljeni januarja 2022

22	**Tip in naslov usposabljanja:**	**prilagojeno usposabljanje**
	Ponudnik (ime in URL):	**VitalIT, German Vitali s. p.** www.vitalit.si/sl/it-trainings/
	Vsebina:	Imamo bogate izkušnje z zagotavljanjem storitev za končne uporabnike, strokovnjake IT in revizorje IT, ki izboljšujejo svoje zmogljivosti na podlagi naslednje generacije orodij ITGC, orodij za spremljanje in varnost. Pristop naših trenerjev je popolnoma prilagojen vašim potrebam in se lahko napaja iz Microsoftovih uradnih tečajev, ki vam pomagajo pridobiti uradno potrdilo o Microsoftovem usposabljanju in si prizadevati za naslednje Microsoftovo uradno potrdilo v sodelovanju z lokalnim Microsoftom Centri za usposabljanje. Pokazali vam bomo pot do znanja in certificiranja.
	Dolžina:	Ni podatka
	Cena:	Ni podatka, potrebno jih je kontaktirati
		Podatki, pridobljeni januarja 2022
23	**Tip in naslov usposabljanja:**	**delavnica - Varnost za programerje**
	Ponudnik (ime in URL):	**CARBOSEC d. o. o.** www.carbonsec.com/sl/izobrazevanje/varnost-za-programerje/
	Vsebina:	Programerji imajo kot graditelji aplikacije v rokah tudi škarje in platno za njeno odpornost pred hekerji. Žal večina programerjev nima ustreznega znanja, da bi proizvedli kodo na varen način. V ta namen je v cikel razvoja aplikacije vključeno varnostno preverjanje, ki sicer pomaga, vendar je takšen način zagotavljanja varnosti v kodi izredno zamuden. Rešitev je dodatno specializirano usposabljanje programerjev, da bodo znali kodo napisati na varen način že v samem začetku. Posledično bo v varnostnem preverjanju ugotovljenih pomanjkljivosti veliko manj in zato celoten proces varne izgradnje aplikacije hitrejši. **Ključne pridobitve:** - Demonstracija izrab najpogostejših ranljivosti na realnih primerih - Priporočila, kako kodo sestaviti na varen način - Praktično sodelovanje slušateljev z mentorjem
	Dolžina:	2 dni
	Cena:	Ni podatka
		Podatki, pridobljeni januarja 2022
24	**Tip in naslov usposabljanja:**	**delavnica – Purple team Coaching**
	Ponudnik (ime in URL):	**CARBOSEC d. o. o.** **www.carbonsec.com/sl/izobrazevanje/purple-team-coaching/**
	Vsebina:	Poskrbeli ste za dobro varnostno vidljivost, nad vašim IT-jem bdi ekipa varnostnih analitikov, specializirana ekipa je pripravljena na takojšen odziv. Manjka le še trenutek resnice – hitra zaznava in odziv na pravi kibernetski napad. Carbonsec-ovi strokovnjaki na podlagi dolgoletnih izkušenj s področja ofenzivne varnosti ter s pomočjo state-of-the-art BAS in

		APT orodij preverjajo učinkovitost varnostnega programa in usmerjajo SOC osebje z namenom izboljševanja ekpertize v vsaki fazi posameznega napada. **Ključne pridobitve:** - Testiranje v skladu z MITRE ATT&CK - Tesno sodelovanje ekip (Red, Blue in IR), korak po koraku - Testiranje podprto z najnovejšo tehnologijo za realne rezultate - Uporaba taktik, tehnik in procedur, ki so relevatni za vašo industrijo - Pridobitev strateških priporočil za izboljšavo tehnologije in procesov
	Dolžina:	Ni podatka
	Cena:	Ni podatka
		Podatki, pridobljeni januarja 2022
25	**Tip in naslov usposabljanja:**	**izobraževanje – Prepoznavanje groženj, ki jih srečamo v okviru informacijske varnosti**
	Ponudnik (ime in URL):	**Fakulteta za računalništvo in informatiko, Univerza v Ljubljani** www.akademijafri.si/izobrazevanja/za-podjetja/prepoznavanje_grozenj_ki_jih_srecamo_v_okviru_informacijske_varnosti/
	Vsebina:	- Osnovno izrazoslovje (INFOSEC, OSINT, modeli groženj, vektorji napada …). - Splošni modeli groženj (potek napadov, pridobljene koristi, profili napadalcev, mehanska in človeška informacijska varnost). - Tipični praktični primeri uspešnih napadov in prepoznavanje le-teh. - Odgovorno razkrivanje incidenta in komunikacija s tehničnim osebjem in pristojnimi organi (npr. SI-CERT). - Pravni okvirji informacijske varnosti za telebane.
	Dolžina:	4 šolske ure
	Cena:	Ni podatka
		Podatki, pridobljeni januarja 2022
26	**Tip in naslov usposabljanja:**	**izobraževanje – Prepoznavanje in odzivanje na InfoSec napade**
	Ponudnik (ime in URL):	**Fakulteta za računalništvo in informatiko, Univerza v Ljubljani** www.akademijafri.si/izobrazevanja/za-podjetja/prepoznavanje_in_odzivanje_na_infosec_napade/
	Vsebina:	- Osvežitev izrazoslovja. - Varovanje podjetja pred napadom (OSINT, penetracijsko testiranje lastne infrastrukture, baze podatkov o vdorih, sodelovanje s CERTi, stalno posodabljanje znanja, posodabljanje strojne in programske opreme, razvoj varnostnih politik, primeri dobre prakse …). - Prepoznavanje incidentov (pregled netflow dnevnikov, etično sledenje napadu, uporaba namenskih spletnih strani, ki analizirajo napade …).

		- Odzivi na napade znotraj pravnih okvirjev - kako zaustaviti napadalce in pri tem ne končati v ječi, ker smo mi kršili zakonodajo? - Komunikacija z nadrejenimi o incidentu in njegovih posledicah. - Svetovanje pravnim in PR službam ter službi, ki skrbi za človeške vire. - Komunikacija s prijaviteljem napada. - Odgovorno razkrivanje napadov (i. e. Responsible disclosure).
	Dolžina:	8 šolskih ur
	Cena:	Ni podatka
		Podatki, pridobljeni januarja 2022
27	**Tip in naslov usposabljanja:**	**izobraževanje – Spustimo tigre na pašo! (Praktična aplikacija računalniške varnosti za podjetja)**
	Ponudnik (ime in URL):	**Fakulteta za računalništvo in informatiko, Univerza v Ljubljani** www.akademijafri.si/izobrazevanja/za-podjetja/spustimo_tigre_na_paso_prakticna_aplikacija_racunalniske_varnosti_za_podjetja/
	Vsebina:	- Usvojili boste temelje varnostne etike in razumeli, v kateri točki bi nadaljevanje njihovega početja brez dovoljenja pomenilo kršenje zakona in imelo neprijetne posledice zanje in njihovega zaposlovalca. - Naučili se boste osnov dela z nekaterimi tipičnimi orodji, ki jih uporabljajo varnostni delavci. - Naučili se boste osnovnih tehnik zbiranja informacij o tarčah, ki jih bomo preverjali. - Znali boste izdelati poročilo o vdoru, skupaj z dobrimi praksami oblikovanja poročil in dokumentacije. - Med trajanjem programa in še nekaj mesecev po njem boste imeli dostop do nekaterih orodij, ki jih uporabljamo pri penetracijskem testiranju.
	Dolžina:	4 x 5 šolskih ur
	Cena:	Ni podatka
		Podatki, pridobljeni januarja 2022

6 Pregled digitalnih kompetenc, ki bi bile potrebne za strokovnjake kibernetske varnosti

6.1 Pregled ogrodij znanj in kompetenc kibernetske varnosti

V tem poglavju bomo na hitro predstavili različna ogrodja kompetenc kibernetske varnosti, ki obstajajo. Iz tega nabora bomo tudi izbrali najbolj primerno ogrodje na podlagi katerega bomo razporejali znanja in kompetence v nadaljevanju projektnih aktivnosti.

Obstaja nekaj različnih ogrodij, ki definirajo znanja in kompetence kibernetske varnosti:

- Cybersecurity Curricula 2017[5]: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, Joint Task Force on Cybersecurity Education
- National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework[6], National Institute of Standards and Technology (NIST)
- A Proposal for a European Cybersecurity Taxonomy[7], Joint Research Centre (JRC)
- CyBOK - The Cyber Security Body of Knowledge[8], The National Cyber Security Centre 2021
- CIISec Skills Framework[9], Charted Institute of Information Security
- ASD Cyber Skills Framework[10], Australian Signals Directorate (ASD)

Cybersecurity Curricula 2017 poleg priporočil za visokošolsko izobraževanje na področju kibernetske varnosti vsebuje tudi ogrodje področij in znanj kibernetske varnosti. Pri njegovi izdelavi so sodelovali ACM, IEEE-CS, IS SIGSEC in FIP WG 11.8. Ogrodje opredeljuje celovit nabor tako imenovanih enot znanja o kibernetski varnosti, združenih v področja znanja. Okvir vključuje tudi možnosti za podporo pri raziskovanju povezav med področji in temami ter za podporo pri določanju disciplin, na katerih je mogoče razviti izobraževalne programe za kibernetsko varnost.

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (slo. Nacionalna pobuda za izobraževanje o kibernetski varnosti Ogrodje deloven sile v kibernetski varnosti) je razvil Nacionalni inštitut za standarde in tehnologijo Združenih držav Amerike v sodelovanju z drugimi partnerji iz akademskega, industrijskega in vladnega sektorja. Osnovni namen je bil zagotoviti skupno izrazoslovje oz. razumevanje konceptov kibernetske varnosti za dosledno in jasno obveščanje o delu na področju kibernetske varnosti in o znanjih in spretnostih kibernetske delovne sile. Ogrodje je razdeljeno v kategorije dela, ki so nato razdeljene v strokovna področja, ki se zatem delijo še na delovne vloge. Vsaka delovna vloga vsebuje opis tipičnih nalog, znanj, spretnosti in veščin.

V okviru cilja Evropske komisije za vzpostavitev mreže kompetenčnih centrov za kibernetsko varnost je Skupno raziskovalno središče (ang. Joint Research Centre) pripravilo študijo o uskladitvi terminologije, opredelitev in področij kibernetske varnosti z nazivom A Proposal for a European Cybersecurity Taxonomy (slo. Predlog evropske taksonomije kibernetske varnosti). Študija predlaga skupno taksonomijo, ki upošteva različne razsežnosti področja kibernetske varnosti. Te so raziskovalno področje (področja znanja, povezana z različnimi vidiki kibernetske varnosti vključno s človeškimi, pravnimi, etičnimi in tehnološkimi vidiki), sektorji gospodarstva, za katere je kibernetska varnost posebej pomembna (imajo potrebo po upoštevanju različnih

[5] https://cybered.acm.org/
[6] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center
[7] https://publications.jrc.ec.europa.eu/repository/handle/JRC118089
[8] https://www.cybok.org/
[9] https://www.ciisec.org/CIISEC/News/CIISec_release_the_latest_version_of_the_Skills_Framework_V_2_4.aspx
[10] https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework

zahtev in/ali izzivov kibernetske varnosti s človeškega, pravnega in/ali etičnega vidika), in tehnologije in primeri uporabe (tehnološke rešitve za krepitev razvoja).

Cyber Security Body of Knowledge (CyBOK) je izdelal Nacionalni center za kibernetsko varnost Združenega kraljestva Velike Britanije in Severne Irske. CyBOK je vodnik po zbirki znanj kibernetske varnosti. Namen je umestitev uveljavljenega znanja v celoten pregled kibernetske varnosti. Skupno CyBOK trenutno zajema 21 področjih znanja, ki so potem razdelana v veliko bolj podrobne enote. Te niso samo naštete oz. zelo na kratko opisane, kot je tipično za podobna ogrodja, ampak so opisane v veliko večje podrobnosti.

CIISec Skills Framework, ki ga je izdelal Charted Institute of Information Security, je podobno kot ogrodje NICE usmerjeno predvsem v kompetence delovne sile. Sama področja kibernetske varnosti (ki jih imenujejo discipline) so sicer v primerjavi z drugimi ogrodji samo na grobo opredeljena, vendar CIISec ogrodje vključuje tudi šest ravni za vsako od disciplin. Ravni spretnosti določijo koliko znanja oz. kompetenc iz posamezne discipline mora vloga v kibernetski varnosti posedovati za svoje delo.

ASD Cyber Skills Framework, je izdal Avstralski direktorat za signale (ang. Australian Signals Directorate) za namene ocenjevanje, vzdrževanje in spremljanje spretnosti ter znanja svojih zaposlenih. ASD Cyber Skills Framework je delno osnovan na CIISec ogrodju spretnosti. ASD ogrodje definira devet vlog kibernetske varnosti, ki so pomembna za direktorat. Ogrodje definira katera znanja in na kakšni ravni so pomembna za posamezne prej opredeljene vloge v organizaciji. ASD Cyber Skills Framework je zato zelo specifičen in ni splošno uporaben, vendar daje dober primer, kako lahko druge organizacije definirajo lastne potrebe po znanju in kompetencah svojih zaposlenih na področju kibernetske varnosti.

6.2 Izbrano ogrodje znanj in kompetenc kibernetske varnosti

Po pregledu obstoječih ogrodij, ki poizkušajo kvalificirati vse kompetence in znanja iz področja kibernetske varnosti smo se odločili, da je za namene te analize najbolj primeren Cybersecurity Curricular Framework in v njem definirana področja in enote znanja (ang. knowledge areas/units), ki je bil izdan kot del poročila Cybersecurity Curricula 2017.

To klasifikacijo smo izbrali iz več razlogov. Klasifikacija je zelo dobro dokumentirana in ena bolj celovitih, ker vsebuje vsa področja, ki bi jih v takšni klasifikaciji pričakovali. Čeprav klasifikacija omogoča zelo dober globalni pregled preko osmih glavnih področij znanja, je tudi granularna, saj se glavna področja nadaljnjo razdelijo na 55 enot znanja, ki se nato še dodatno razdelijo na 288 tematik, vsaka od katerih je tudi opisana. Klasifikacija vsebine študijskih predmetov in certifikatov je bila narejena na podlagi tematik in njihovih opisov, vendar smo vsebine razporedili samo v enote znanja. Poln seznam področij in enot znanja je naveden v Tabela 4. Na podlagi te klasifikacije smo v nadaljevanju razporejali znanja, pridobljena na različnih študijskih programih (oz. pri posameznih predmetih na programu) in certifikatih iz področja kibernetske varnosti.

Tabela 4: Področja in enote znanja uporabljeni za klasifikacijo vsebin študijskih predmetov in certifikatov.

Področja znanja	Enote znanja	
Varnost podatkov (ang. Data Security)	Kriptografija (ang. Cryptography)	Digitalna forenzika (ang. Digital Forensics)
	Celovitost in overjanje (ang. Data Integrity and Authentication)	Nadzor dostopa (ang. Access Control)

	Varni komunikacijski protokoli (ang. Secure Communication Protocols)	Kriptoanaliza (ang. Cryptanalysis)
	Zasebnost podatkov (ang. Data Privacy)	Varnost shranjevanja informacij (ang. Information Storage Security)
Varnost programske opreme (ang. Software Security)	Temeljna načela (ang. Fundamental Principles)	Zasnova/načrtovanje (ang. Design)
	Implementacija (ang. Implementation)	Analiza in testiranje (ang. Analysis and Testing)
	Postavitev in vzdrževanje (ang. Deployment and Maintenance)	Dokumentiranje (ang. Documentation)
	Etika (ang. Ethics)	
Varnost komponent (ang. Component Security)	Zasnova komponent (ang. Component Design)	Nabava komponent (ang. Component Procurement)
	Testiranje komponent (ang. Component Testing)	Obratni (ali povratni) inženiring komponent (ang. Component Reverse Engineering)
Varnost povezave (ang. Connection Security)	Fizični mediji (ang. Physical Media)	Fizični vmesniki in priključki (ang. Physical Interfaces and Connectors)
	Arhitektura strojne opreme (ang. Hardware Architecture)	Arhitektura porazdeljenih sistemov (ang. Distributed Systems Architecture)
	Arhitektura omrežij (ang. Network Architecture)	Implementacija omrežij (ang. Network Implementations)
	Omrežne storitve (ang. Network Services)	Obramba omrežij (ang. Network Defense)
Varnost sistemov (ang. System Security)	Sistemsko razmišljanje (ang. System Thinking)	Upravljanje sistemov (ang. System Management)
	Sistemski dostop (ang. System Access)	Nadzor sistemov (ang. System Control)
	Upokojevanje sistemov (ang. System Retirement)	Testiranje sistemov (ang. System Testing)
	Tipične arhitekture sistemov (ang. Common System Architectures)	
Človeški vidik varnosti (ang. Human Security)	Upravljanje identitet (ang. Identity Management)	Socialni inženiring (ang. Social Engineering)

	Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti (ang. Personal Compliance with Cybersecurity Rules/Policy/ Ethical Norms)	Osveščenost (ali zavedanje) in razumevanje (ang. Awareness and Understanding)
	Družbena in vedenjska zasebnost (ang. Social and Behavioral Privacy)	Zasebnost in varnost osebnih podatkov (ang. Personal Data Privacy and Security)
	Uporabna varnost in zasebnost (ang. Usable Security and Privacy)	
Organizacijska varnost (ang. Organizational Security)	Upravljanje tveganj (ang. Risk Management)	Varnostno upravljanje in politika (ang. Security Governance & Policy)
	Analitična orodja (ang. Analytical Tools)	Upravljanje sistemov (ang. Systems Administration)
	Načrtovanje kibernetske varnosti (ang. Cybersecurity Planning)	Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov (ang. Business Continuity, Disaster Recovery, and Incident Management)
	Upravljanje varnostnih programov (ang. Security Program Management)	Varnost osebja (ang. Personnel Security)
	Varnostne operacije (ang. Security Operations)	
Družbena varnost (ang. Societal Security)	Kibernetski kriminal (ang. Cybercrime)	Kibernetsko pravo (ang. Cyber Law)
	Kibernetska etika (ang. Cyber Ethics)	Kibernetska politika (ang. Cyber Policy)
	Zasebnost (ang. Privacy)	

6.3 Analiza pomembnosti kompetenc na podlagi študijskih programov

Različni profili delovnih nalog potrebujejo različna znanja in določena znanja so veliko bolj iskana oz. se potrebujejo v večji količini. Zato je pri oblikovanju izobraževalnega programa pomembno upoštevati te dejavnike in temu primerno prilagoditi vsebino študijskega programa ali usposabljanja.

Z analizo študijskih programov smo želeli ugotoviti, katere vsebine, ki pokrivajo kibernetsko varnost, se predavajo na študijskih programih. Takšne študijske programe smo črpali iz CYBERHEAD (ang. Cybersecurity Higher Education Database) zbirke visokošolskih študijskih

programov na področju kibernetske varnosti v Evropi, ki ga upravlja Evropska agencija za kibernetsko varnost - ENISA (ang. European Union Agency for Cybersecurity). Zbirka trenutno vključuje 126 dodiplomskih in magistrskih programov. Iz te zbirke smo izbrali naključen vzorec dvanajstih študijskih programov, ki predstavlja skoraj deset odstotkov celotne zbirke. Edini omejujoč faktor, ki smo ga pri izboru upoštevali, je dostopnost predmetnikov in podrobnejši opisi posameznih predmetov, na podlagi katerih smo lahko predmete razvrščali v prej predstavljeno klasifikacijo (glej Tabela 4). Izbranih dvanajst študijskih programov, je predstavljenih v Tabela 5. V tabeli so vključeni imena programov (v angleščini, kot ga sami navajajo), izobraževalne ustanove (v angleščini), stopnje študija, povezave do študijskega programa in ECTS (ang. European Credit Transfer System) točke. ECTS točke, navedene zunaj oklepaja, predstavljajo vrednost ECTS točk, ki jih študent potrebuje za zaključek posameznega študijskega programa, medtem ko je vrednost v oklepaju seštevek ECTS točk vseh predmetov, ki smo jih ovrednotili za posamezen študijski program. Med obema vrednostnima je lahko velika razlika, če študijski program samo delno ponuja vsebine iz kibernetske varnosti (npr. multidisciplinarni študijski program) ali če program vsebuje oz. ponuja veliko izbirnih vsebin (študentom v takšnih primerih, ni potrebno obiskovati vseh predmetov, ki so na voljo). Za namene te analize smo skupno ovrednotili oz. klasificirali vsebine iz 184 različnih predmetov, ki skupaj predstavljajo 896 točk ECTS.

Tabela 5: Seznam študijskih programov, katerih predmete smo klasificirali glede na njihovo vsebino iz področja kibernetske varnosti.

Program:	Business Information Technology, Cyber Security	
Univerza:	Laurea University of Applied Sciences (Finska)	
Stopnja:	Dodiplomski študij	ECTS: 210 (45)
Povezava:	https://www.laurea.fi/en/degree_programmes/business-management-and-information-technology/bit-cyber-security/	
Program:	Program: Information & Cyber Security	
Univerza:	Univerza: Lucerne University of Applied Sciences and Arts (Švica)	
Stopnja:	Stopnja: Dodiplomski študij	ECTS: 180 (78)
Povezava:	https://www.hslu.ch/en/lucerne-school-of-information-technology/degree-programs/bachelor/information-and-cyber-security/	
Program:	Program: Cybersecurity	
Univerza:	Univerza: Masaryk University (Češka)	
Stopnja:	Stopnja: Dodiplomski študij	ECTS: 180 (54)
Povezava:	https://www.muni.cz/en/bachelors-and-masters-study-programmes/26540-cybersecurity	
Program:	Program: Cyber Security	
Univerza:	Univerza: ETH Zurich (Švica)	
Stopnja:	Stopnja: Magistrski študij	ECTS: 120 (89)
Povezava:	https://inf.ethz.ch/studies/master/master-cybsec.html	
Program:	Program: Cybersecurity Management	
Univerza:	Univerza: BA School of Business and Finance (Latvija)	
Stopnja:	Stopnja: Magistrski študij	ECTS: 120 (57)
Povezava:	https://www.ba.lv/studies/program/cybersecurity-management/	
Program:	Program: Information Security	
Univerza:	Univerza: University College London (Združeno kraljestvo Velike Britanije in Severne Irske)	
Stopnja:	Stopnja: Magistrski študij	ECTS: 90 (90) ≅ 180 credits

Povezava:	https://www.ucl.ac.uk/prospective-students/graduate/taught-degrees/information-security-msc
Program:	Program: IT security
Univerza:	Univerza: TU Darmstadt (Nemčija)
Stopnja:	Stopnja: Magistrski študij ECTS: 120 (196)
Povezava:	https://www.tu-darmstadt.de/studieren/studieninteressierte/studienangebot_studiengaenge/studiengang_183744.en.jsp
Program:	Program: Cyber Security
Univerza:	Univerza: JAMK University of Applied Science (Finska)
Stopnja:	Stopnja: Magistrski študij ECTS: 60 (20)
Povezava:	https://www.jamk.fi/en/Education/Technology-and-Transport/Cyber-Security-Masters-Degree/
Program:	Program: Master in Cybersecurity
Univerza:	Univerza: University of Aveiro (Portugalska)
Stopnja:	Stopnja: Magistrski študij ECTS: 120 (84)
Povezava:	https://www.ua.pt/en/curso/462
Program:	Program: Cybersecurity
Univerza:	Univerza: International Hellenic University (Grčija)
Stopnja:	Stopnja: Magistrski študij ECTS: 60 (54)
Povezava:	https://www.ihu.gr/ucips/postgraduate-programmes/cybersecurity
Program:	Program: IT security
Univerza:	Univerza: University of Applied Sciences Vienna (Austrija)
Stopnja:	Stopnja: Magistrski študij ECTS: 120 (89)
Povezava:	https://www.fh-campuswien.ac.at/en/studies/study-courses/detail/it-security-master.html
Program:	Program: IT & Mobile Security
Univerza:	Univerza: FH JOANNEUM University of Applied Sciences (Austrija)
Stopnja:	Stopnja: Magistrski študij ECTS: 120 (40)
Povezava:	https://www.fh-joanneum.at/it-und-mobile-security/master/en/my-studies/curriculum/

Postopek ocenjevanja enot znanja, ki jih posamezen predmet pokriva, smo izvedli na podlagi opisov predmetov. Za vsak predmet iz kibernetske varnosti v vsakem študijskem programu smo označili znanja, ki so del te učne enote. Merjenje pomembnosti vsakega področja oz. enote znanja smo ocenili na podlagi točkovanja pogostosti teh vsebin. Vsak predmet ima eno točko, ki se enakovredno razporedi med vse enote znanja (področja znanja pridobijo točke, tako da se združijo točke vseh enot, ki pripadajo v posamezno področje znanja). To pomeni, da več znanj kot predmet vsebuje, manjši delež te točke pripada posamezni enoti znanja, ki jo predmet vsebuje. Posledično bolj splošni predmeti prispevajo manjši deleže točke velikemu številu znanj in zelo usmerjeni oz. specializirani predmeti prispevajo velik delež točke majhnemu številu znanj (ker je to bolj podrobno, kot v primeru splošnih predmetov). Izračun ECTS točk sledi istemu postopku, le da je končni delež točke, ki jo posamezna enota znanja prejme normiran glede na ECTS točke predmeta (tj. pomnožen s številom ECTS točk predmeta). Takšna normalizacija je bila uvedena, ker smo želeli upoštevati, da predmeta, ki imata npr. 2 oziroma 10 ECTS točk in pokrivata iste enote znanja, storita to na dveh različnih nivojih, kjer je drugi predmet predvidoma veliko bolj podroben in detajlen pri razlagi teh znanj, kot prvi predmet, ki od študentov zahteva veliko manj

časa in truda. Iz tega razloga bomo tudi smatrali te rezultate kot bolj reprezentativne in jim bomo dali prednost pred nenormiranim točkovanjem.

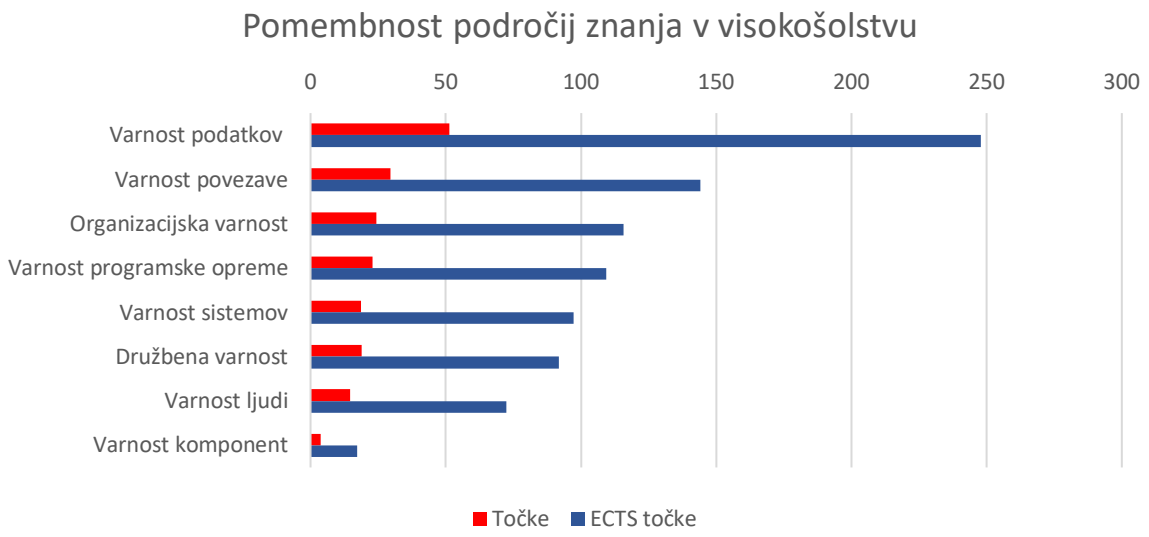
V Tabela 6 so predstavljeni rezultati meritev vključenosti področij znanja v študijske predmete. V levi polovici so področja razporejena glede na točke v desni pa so normirana glede na ECTS točke, od najbolj pogostih vsebin do najmanj pogostih. Vidimo, da med obema metodama merjenja ni velikih razlik v vrstnem redu najpogosteje obravnavanih področij znanja. Edina razlika je v petem in šestem mestu, kjer si mesti izmenjata Družbena varnost in Varnost sistemov. To pokažejo tudi razmerja med ECTS točkami in nenormiranimi točkami, kjer so razmerja za vsa področja znanja med 4,69 (področje ima 4,69-krat toliko ECTS točk, kot ima Točk) in 5,23, kar ni veliko. Največje razmerje ima, prav Varnost sistemov, ki zaradi tega, na ECTS lestvici pridobi eno mesto, najmanjše razmerje pa je pri Varnosti komponent, ki pa je tudi na splošno očitno najmanj pokrito področje v izobraževanju.

Tabela 6: Meritve vključenosti področij znanja kibernetske varnosti v visokošolske vsebine

#	Točke	Področje znanja	Področje znanja	ECTS točke
1	51,37	Varnost podatkov	Varnost podatkov	247,97
2	29,45	Varnost povezave	Varnost povezave	144,14
3	24,35	Organizacijska varnost	Organizacijska varnost	115,72
4	23,00	Varnost programske opreme	Varnost programske opreme	109,39
5	18,89	Družbena varnost	Varnost sistemov	97,21
6	18,58	Varnost sistemov	Družbena varnost	91,85
7	14,70	Varnost ljudi	Varnost ljudi	72,48
8	3,67	Varnost komponent	Varnost komponent	17,23

Na Slika 3 so ponovno prikazani isti podatki, vendar tokrat v grafični obliki (razporejen glede na ECTS točke). Iz slike je očitno, da je področje znanja, ki mu visokošolska izobraževanja na področju kibernetske varnosti namenjajo največ pozornosti in je posledično predvidoma najbolj pomembno Varnost podatkov. Varnost podatkov je skoraj pričakovano doseglo največ točk, ker podatki so osnoven blok vseh informacijskih sistemov in njihova varnost je posledično ključnega pomena za kakršnokoli varno okolje. Ostala področja si zatem sledijo z relativno enakomerno razliko med njimi z izjemo povsem zadnjega področja Varnosti komponent, ki je očitno najslabše

zastopano v visokošolskem izobraževanju. Ena razlaga za to, je zagotovo, da je varnost komponent relativno majhno področje (vsebuje samo 4 enote znanja), ki je istočasno tudi zelo specifično.



Slika 3: Grafikon pomembnosti področij znanja v visokošolskem izobraževanju kibernetske varnosti.

V Tabela 7 so prikazani rezultati za posamezne enote znanja (obarvane enako kot področje znanja v katero spadajo iz *Tabela 6*). Rezultati za enote znanja so veliko bolj relevantni za analizo pomembnosti kompetenc oz. znanj na področju kibernetske varnosti in njenega izobraževanja, ker gre za manjše bolj usmerjene enote. V rezultatih za področja znanja je Organizacijska varnost (obarvana rdeče) zasedla tretje mesto po pomembnosti. V neki meri je to zato, ker to področje vsebuje največ (9) enot znanja, ki prispevajo k oceni tega področja. V Tabela 7 namreč lahko vidimo, da enote obarvane rdeče niso v samem vrhu in nekaj jih je zelo nizko v seznamu. Tukaj tudi vidimo, da za razliko od področij znanja, tukaj prišlo do precej razlik v zaporedju pomembnosti enot znanja glede na način merjenja (Točke v primerjavi z ECTS točkami). Na prvih dveh mestih sta suvereno uvrščena Kriptografija in Obramba omrežij, zatem pa se vrstni red pomembnosti v veliki meri razlikuje. To potrjujejo tudi razmerja med obema načinoma točkovanja. Med enotami znanja je najmanjše razmerje med ECTS točkami in nenormiranim točkovanjem (če izpustimo enote, ki niso bile naslonjene v nobenem od zajetih študijskih programov) 2,8 (Dokumentiranje), medtem ko je največje 7,16 (Socialni inženiring). V sami razporeditvi pomembnosti enot znanja se sicer to odraža v večinoma majhnih razlikah, vendar so nekateri primeri bolj signifikantni. Na primer, Tipične arhitekture sistemov so v ECTS točkovanju 12 mest nižje in Digitalna forenzika je 9 mest nižje, medtem ko je Varni komunikacijski protokoli v ECTS točkovanju uvrščeno 8 mest višje. To v neki meri nakazuje, da sta prvi dve enoti znanja tipično naslovljeni v manj zahtevnih predmetih (tj. predmetih z manj ECTS točkami), medtem ko so Varni komunikacijski protokoli predmet bolj obsežnih učnih enot. Povsem na dnu tabele vidimo, da dve enoti znanja (Nabava komponent in Upokojevanje sistemov) nista bili naslonjeni v nobenem predmetu nobenega od študijskih programov, ki smo jih zajeli v raziskavi. Temu je najverjetneje tako, ker gre za dve zalo specifični enoti znanja, ki so relevantne v zelo majhnem okviru časa in/ali za zelo majhno število delovnih mest.

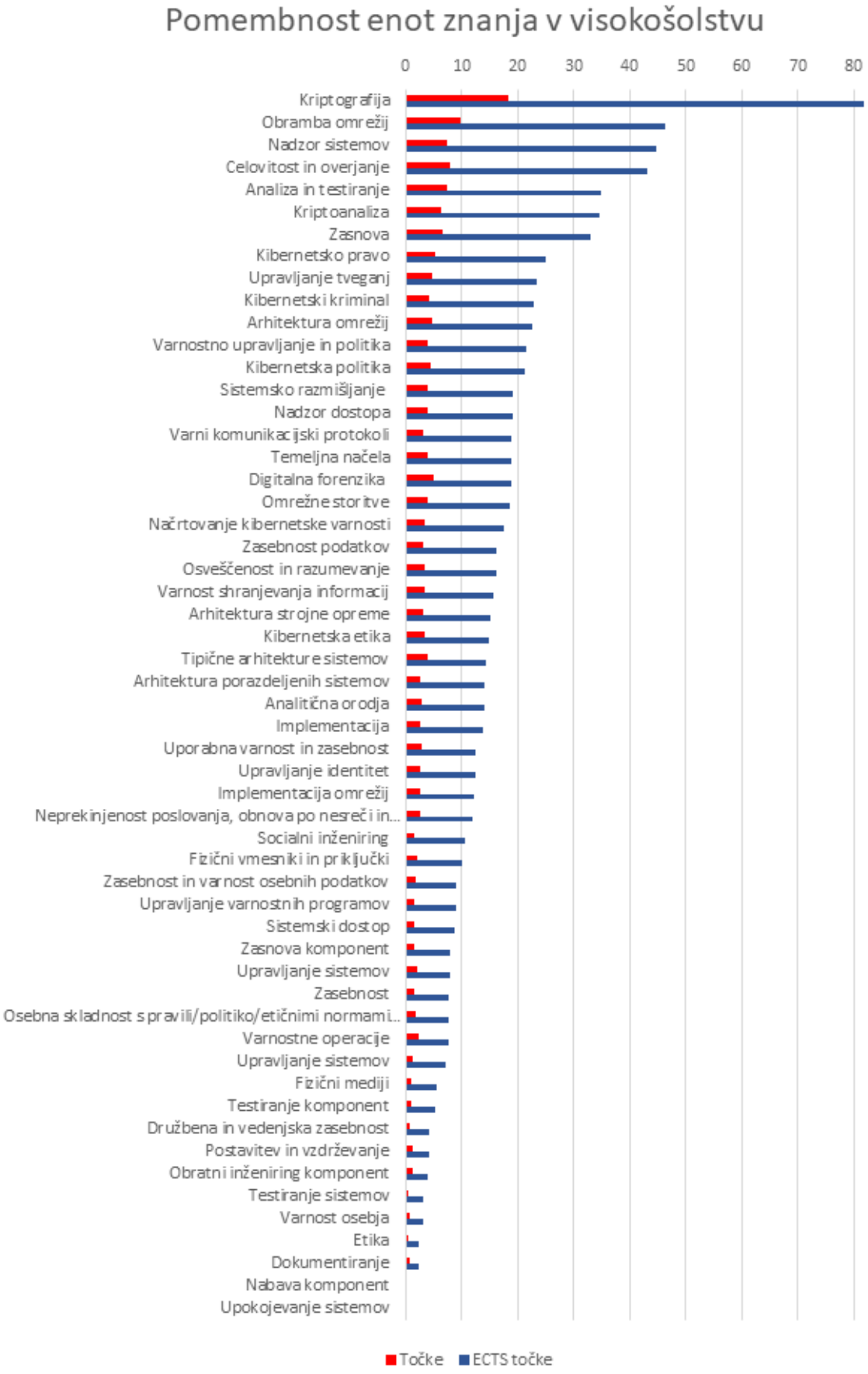
Tabela 7: Meritve vključenosti enot znanja kibernetske varnosti v visokošolske vsebine

#	Točke:	Enote znanja	Enote znanja	ECTS točke
1	18,28	Kriptografija	Kriptografija	81,72

2	9,79	Obramba omrežij	Obramba omrežij	46,17
3	7,88	Celovitost in overjanje	Nadzor sistemov	44,58
4	7,41	Analiza in testiranje	Celovitost in overjanje	43,01
5	7,34	Nadzor sistemov	Analiza in testiranje	34,85
6	6,56	Zasnova	Kriptoanaliza	34,58
7	6,40	Kriptoanaliza	Zasnova	33,02
8	5,16	Kibernetsko pravo	Kibernetsko pravo	24,91
9	4,97	Digitalna forenzika	Upravljanje tveganj	23,37
10	4,86	Upravljanje tveganj	Kibernetski kriminal	22,90
11	4,65	Arhitektura omrežij	Arhitektura omrežij	22,46
12	4,50	kibernetska politika	Varnostno upravljanje in politika	21,41
13	4,32	Kibernetski kriminal	kibernetska politika	21,37
14	4,07	Tipične arhitekture sistemov	Sistemsko razmišljanje	19,19
15	4,06	Nadzor dostopa	Nadzor dostopa	19,14
16	4,02	Sistemsko razmišljanje	Varni komunikacijski protokoli	18,95
17	3,99	Varnostno upravljanje in politika	Temeljna načela	18,80
18	3,94	Temeljna načela	Digitalna forenzika	18,78
19	3,81	Omrežne storitve	Omrežne storitve	18,46
20	3,46	Varnost shranjevanja informacij	Načrtovanje kibernetske varnosti	17,53
21	3,41	Načrtovanje kibernetske varnosti	Zasebnost podatkov	16,21
22	3,32	Kibernetska etika	Osveščenost in razumevanje	16,13
23	3,31	Osveščenost in razumevanje	Varnost shranjevanja informacij	15,59
24	3,24	Varni komunikacijski protokoli	Arhitektura strojne opreme	15,13
25	3,07	Zasebnost podatkov	Kibernetska etika	14,90
26	3,03	Arhitektura strojne opreme	Tipične arhitekture sistemov	14,34
27	2,86	Analitična orodja	Arhitektura porazdeljenih sistemov	14,13
28	2,75	Uporabna varnost in zasebnost	Analitična orodja	13,96
29	2,69	Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov	Implementacija	13,83
30	2,65	Arhitektura porazdeljenih sistemov	Uporabna varnost in zasebnost	12,42
31	2,65	Upravljanje identitet	Upravljanje identitet	12,34
32	2,52	Implementacija omrežij	Implementacija omrežij	12,21
33	2,51	Implementacija	Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov	11,84
34	2,39	Varnostne operacije	Socialni inženiring	10,51
35	2,06	Fizični vmesniki in priključki	Fizični vmesniki in priključki	10,12
36	2,03	Upravljanje sistemov	Zasebnost in varnost osebnih podatkov	9,07
37	1,89	Zasebnost in varnost osebnih podatkov	Upravljanje varnostnih programov	8,93
38	1,79	Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti	Sistemski dostop	8,81
39	1,62	Zasnova komponent	Zasnova komponent	8,06
40	1,59	Zasebnost	Upravljanje sistemov	7,93
41	1,47	Socialni inženiring	Zasebnost	7,77

42	1,43	Upravljanje varnostnih programov	Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti	7,76
43	1,43	Sistemski dostop	Varnostne operacije	7,71
44	1,22	Postavitev in vzdrževanje	Upravljanje sistemov	7,08
45	1,17	Upravljanje sistemov	Fizični mediji	5,46
46	1,17	Obratni inženiring komponent	Testiranje komponent	5,17
47	0,93	Fizični mediji	Družbena in vedenjska zasebnost	4,25
48	0,88	Testiranje komponent	Postavitev in vzdrževanje	4,21
49	0,84	Družbena in vedenjska zasebnost	Obratni inženiring komponent	4,00
50	0,83	Dokumentiranje	Testiranje sistemov	3,21
51	0,68	Varnost osebja	Varnost osebja	3,04
52	0,56	Testiranje sistemov	Etika	2,35
53	0,52	Etika	Dokumentiranje	2,33
54	0,00	Nabava komponent	Nabava komponent	0,00
55	0,00	Upokojevanje sistemov	Upokojevanje sistemov	0,00

Slika 4 je ponovno grafični prikaz istih podatkov za enote znanja (razporejen glede na ECTS točke). Ponovno je tudi zelo očitna ena enota znanja, ki izstopa pred drugimi v pogostosti pojavljanja v visokošolskih izobraževalnih programih iz področja kibernetske varnosti. Kriptografija je zbrala skoraj dvakrat toliko točk kot naslednja najbolje zastopana enota znanja. Razlog za to je vseprisotnost tega znanja oz. njegova potreba za razumevanje delovanja večine drugih (tehničnih) varnostnih pristopov. Kriptografiji sledi skupina znanj iz Obrambe omrežij, Nadzora sistemov ter Celovitosti in overjanja. Zatem je ponovno viden razkorak pred naslednjo skupino treh enot znanja, ki so Analiza in testiranje, Kriptoanaliza in Zasnova (varne programske opreme). Zatem sledijo preostale enote znanja, katerih rezultati pomembnosti relativno linearno padajo do že omenjenih Nabave komponent in Upokojevanja sistemov, ki v vzorcu izobraževanj, zajetih v tej raziskavi sploh nista bili naslovljeni.



Slika 4: Grafikon pomembnosti enot znanja v visokošolskem izobraževanju kibernetske varnosti.

6.4 Analiza pomembnosti kompetenc na podlagi certifikatov

Podobno kot za študijske programe smo tudi za ponujene certifikate želeli izvedeti, katere vsebine iz kibernetske varnosti so najbolj zastopane v takšnih izobraževanjih oz. so potrebne za pridobitev certifikatov. V analizo smo vključili deset najbolj iskanih certifikatov v gospodarstvu, ki smo jih predstavili v 0. poglavju (Tabela 1). Posredno je ta analiza vsebin certificiranj tudi pokazatelj iskanih znanj v gospodarstvu, vendar za Združene Države Ameriki, kjer je bila osnovna analiza najbolj iskanih certifikatov izvedena. Za pomembnost znanj v slovenskem gospodarstvu bomo zato izvedli ločeno in bolj usmerjeno raziskavo.

Posamezne certifikate smo klasificirali v različna področja znanja glede na prosto dostopne informacije o samih certifikatih in iz vsebin različnih izobraževanj, ki so tipično ponujena kot priprava (ali celo pogoj) za pristop k opravljanju certifikata. Merjenje pomembnosti vsakega področja oz. enote znanja smo, tako kot pri študijskih programih, ocenili na podlagi točkovanja pogostosti teh vsebin. Vsak certifikat ima eno točko, ki se enakovredno razporedi med vse enote znanja. Te točke se seštejejo za vrednosti področij znanja.

V Tabela 8 so prikazani rezultati za področja znanj. Tako kot pri visokošolskem izobraževanju, je na prvem mestu Varnost podatkov, čeprav ta ni več tako dominantno na prvem mestu, kot je bila pri visokošolskem izobraževanju. Sledi Organizacijska varnost, kar je v neki meri pričakovano, saj takšne oblike certificiranj tipično podpirajo večje organizacije in posledično, vsebujejo poudarek na tem kako organizirati varovanje, predvideti tveganja itd. Naslednja je Varnost povezave, ki je bila pri merjenju visokošolskih izobraževalnih programov druga. Edina druga zanimiva sprememba s prejšnjo analizo je Varnost programske opreme, ki je padlo iz četrtega na sedmo mesto. Razloge vidimo predvsem v tem, da vključeni certifikati (in če pogledamo seznam vseh certificiranj, ki smo jih navedli v predhodnem poglavju) niso namenjeni razvoju programske opreme in posledično tega znanja ne potrebujejo, saj ta znanja niso tako univerzalno potrebna kot so npr. znanja iz Varnosti podatkov.

Tabela 8: Meritve vključenosti področij znanja kibernetske varnosti v certifikate

#	Področje znanja	Točke
1	Varnost podatkov	2,5854
2	Organizacijska varnost	2,2003
3	Varnost povezave	1,9161
4	Družbena varnost	1,0969
5	Varnost sistemov	1,0433
6	Varnost ljudi	0,8377
7	Varnost programske opreme	0,1987
8	Varnost komponent	0,1216

Slika 5 še bolj nazorno pokaže, da Varnost podatkov ni več tako dominantno najpomembnejše področje znanja in da sta pri vsebinah certifikatov, področji Varnosti programske opreme in Varnosti komponent naslovljeni v zelo majhnem obsegu.

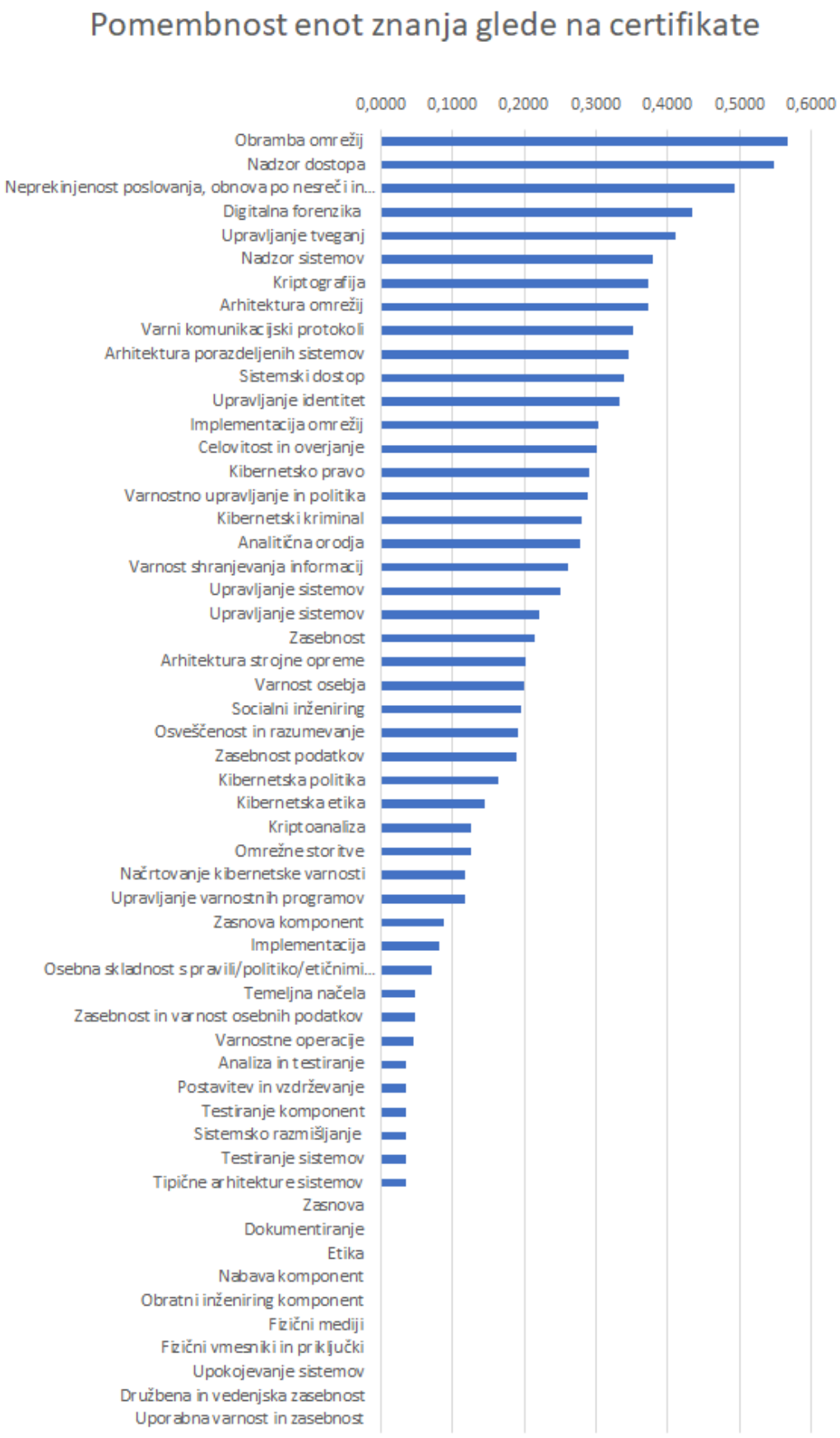
Slika 5:Pomembnost področij znanja glede na certifikate iz kibernetske varnosti

Tabela 9 vsebuje rezultate za vse enote znanja. V tem seznamu opazimo več velikih razlik s seznamom, ki smo ga pridobili na podlagi visokošolskih izobraževalnih programov – npr. Kriptografija je iz absolutnega prvega mesta padla na sedmo mesto, medtem se je Nadzor dostopa povzpel iz petnajstega na drugo mesto. Iz zadnjih zapisov v tabeli in *Slika 6* je tudi razvidno, da je tu veliko več področji, ki niso bila naslovljeni v nobenem od analiziranih certificiranj. Razloge za to vidimo predvsem v dveh razlogih. Prvič, v tej kategoriji bilo ocenjenih veliko manj vsebin kot jih je bilo v predmetih iz visokošolskih izobraževalnih programov in posledično je veliko večja verjetnost da bolj obrobna znanja niso bila zajeta. Drugi razlog pa je zagotovo, da je namen certificiranj izkazati obvladovanje bolj specifičnih znanj, medtem ko so visokošolski programi bolj splošni in namenjeni temu, da opremijo študente s čim širšim naborom znanj, ki jim bodo lahko prišla prav na njihovi profesionalni poti.

Tabela 9: Meritve vključenosti enot znanja kibernetske varnosti v certifikate

#	Enote znanja	Točke
1	Obramba omrežij	0,5660
2	Nadzor dostopa	0,5472
3	Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov	0,4932
4	Digitalna forenzika	0,4344
5	Upravljanje tveganj	0,4099
6	Nadzor sistemov	0,3797
7	Kriptografija	0,3729
8	Arhitektura omrežij	0,3729
9	Varni komunikacijski protokoli	0,3524
10	Arhitektura porazdeljenih sistemov	0,3462
11	Sistemski dostop	0,3390
12	Upravljanje identitet	0,3322
13	Implementacija omrežij	0,3033
14	Celovitost in overjanje	0,3015
15	Kibernetsko pravo	0,2915
16	Varnostno upravljanje in politika	0,2886

17	Kibernetski kriminal	0,2806
18	Analitična orodja	0,2788
19	Varnost shranjevanja informacij	0,2615
20	Upravljanje sistemov	0,2495
21	Upravljanje sistemov	0,2212
22	Zasebnost	0,2144
23	Arhitektura strojne opreme	0,2024
24	Varnost osebja	0,2002
25	Socialni inženiring	0,1951
26	Osveščenost in razumevanje	0,1914
27	Zasebnost podatkov	0,1901
28	kibernetska politika	0,1645
29	Kibernetska etika	0,1459
30	Kriptoanaliza	0,1254
31	Omrežne storitve	0,1254
32	Načrtovanje kibernetske varnosti	0,1178
33	Upravljanje varnostnih programov	0,1169
34	Zasnova komponent	0,0871
35	Implementacija	0,0821
36	Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti	0,0714
37	Temeljna načela	0,0476
38	Zasebnost in varnost osebnih podatkov	0,0476
39	Varnostne operacije	0,0455
40	Analiza in testiranje	0,0345
41	Postavitev in vzdrževanje	0,0345
42	Testiranje komponent	0,0345
43	Sistemsko razmišljanje	0,0345
44	Testiranje sistemov	0,0345
45	Tipične arhitekture sistemov	0,0345
46	Zasnova	0,0000
47	Dokumentiranje	0,0000
48	Etika	0,0000
49	Nabava komponent	0,0000
50	Obratni inženiring komponent	0,0000
51	Fizični mediji	0,0000
52	Fizični vmesniki in priključki	0,0000
53	Upokojevanje sistemov	0,0000
54	Družbena in vedenjska zasebnost	0,0000
55	Uporabna varnost in zasebnost	0,0000



Slika 6: Pomembnost enot znanja glede na certifikate iz kibernetske varnosti

6.5 Ugotovitve in analiza

V raziskavi smo želeli ugotoviti, katera znanja iz kibernetske varnosti so pomembna za vključitev v izobraževalni program (študijski program ali program usposabljanja) kibernetske varnosti, katerih zasnova je tudi cilj tega projekta. V ta namen smo uporabili kot osnovo področja znanja, ki jih definirajo smernice IEEE&ACM in analizirali vsebine že obstoječih študijskih programov in certifikatov iz tega področja z namenom ugotavljanja, katere od področij znanj se največ pojavljajo in pokrivajo. Rezultati bi nam služili kot osnova za gradnjo lastnih predlogov študijskih programov in katalogov izobraževanj, saj bi lahko podali fokus na tista področja znanja, ki so pomembna tako za druge formalne študijske programe kot za, s strani gospodarstva podprta, certificiranja. Metodologijo analize in rezultate smo podrobneje opisali v prejšnjih poglavjih. V grobem sta obe analizi pokazali podobne rezultate, vendar so določene razlike bile očitne. V visokošolskih izobraževalnih programih je očiten razvoj znanj iz nič (začne se z osnovami in gradi na tem) in so na splošno (vsaj ko ne gre za specializirane študijske programe) bolj široko usmerjeni, medtem ko so certifikati tipično bolj specifični in ne zajemajo toliko osnovnih znanj, za katere se mogoče že predvideva, da so udeleženci že seznanjeni z njimi oz. so takšna znanja, predstavljena zelo na hitro. Pri končnem magistrskem programu, ki bo nastal med tem projektom, bi se torej glede vsebin morali bolj nagibati proti razporeditvi vsebin, kot smo jih zaznali v analizi visokošolskih programov, medtem ko bi za program usposabljanja (seveda ob upoštevanju, komu je namenjen) mogoče bilo bolj smiselno upoštevati rezultate analize certifikatov in vključevati več vsebin, ki so se tam izkazale za bolj pomembne, posebej, ker sta tako certificiranje in usposabljanje tipično namenjena bolj specifičnim kompetencam in znanjem, ki so v interesu gospodarstva.

7 Zaključek

Z aktivnostmi prvega delovnega paketa smo želeli pridobiti trdne osnove za nadaljnje analize in končno pripravo predlogov študijskih programov. Izvedli smo preglede številnih področij, ki smo jih podrobno predstavili skozi poglavja tega poročila. Pregledi so bili namenjeni podrobnem spoznavanju trenutnega stanja izobraževanja in usposabljanja kibernetske varnosti, pri čemer pa so analize vključevale bodisi splošne in globalne smernice ali okvirje ter pasivne analize stanja v Sloveniji. S pregledom smo pridobili splošne temelje razumevanja področja izobraževanja kibernetske varnosti, ki pa še ni prilagojen dejanskim potrebam Slovenije. V naslednjem delovnem paketu načrtujemo preveriti razumevanje in potrebo po znanjih in kompetencah s področja kibernetske varnosti s slovenskim gospodarstvom in javno upravo. Rezultati, ki si jih s tem nadejamo bodo tako prvi pokazatelj okvirjev študijskih programov kibernetske varnosti, ki bi bili primerni za slovensko področje in hkrati temeljili na vseh ključnih smernicah, ki za to področje veljajo.

8 Priloga A: Pregled obstoječih študijski programov v Sloveniji, ki vsebujejo module ali smeri, ki naslavljajo področje kibernetske varnosti

Inštitucija	Članica	Program	Stopnja	Modul ali smer	Predmeti
Alma Mater	/	Spletna znanost in tehnologije	Mag	Kibernetska varnost	Informacijske grožnje in upravljanje z incidenti Uvod v digitalno forenziko Uporabna kibernetska varnost Kibernetska varnost v gospodarstvu Kriminaliteta in upravljanje tveganj v digitalni družbi
Univerza v Ljubljani	Fakulteta za računalništvo in informatiko	Računalništvo in informatika	Mag	Omrežja in varnost	Kriptografija in računalniška varnost Informacijska varnost in zasebnost Digitalna forenzika Brezžična senzorska omrežja
Univerza v Mariboru	Fakulteta za elektrotehniko, računalništvo in informatiko	Informatika in tehnologije komuniciranja	Mag	Varnost IS in upravljanje z varnostjo	Napredna informacijska varnost Podatkovna zaščita Zanesljivost in testiranje IS
Univerza v Mariboru	Fakulteta za elektrotehniko, računalništvo in informatiko	Informatika in tehnologije komuniciranja oz. Informatika in podatkovne tehnologije	Uni	Informacijska varnost	Zagotavljanje kakovosti Digitalna forenzika Kibernetska varnost

9 Priloga B: Pregled obstoječih študijski programov in učnih enot v Sloveniji, ki naslavljajo področje kibernetske varnosti in niso del smeri ali modulov s tega področja

Inštitucija	Članica	Program		Predmet	Izbirnost
Alma Mater	/	Spletne in informacijske tehnologije	VS	Uvod v kriptografijo in varnost podatkov Informacijska varnost	Obvezni Izbirni
Alma Mater	/	Arhivistika	VS	Informacijska varnost	Izbirni
B2	/	Poslovna informatika	Visoka	Informacijska varnost	Obvezni
Univerza v Novem Mestu	Fakulteta za Informacijske Študije	Računalništvo in spletne tehnologije	Mag	Kibernetska varnost	Obvezni
Univerza v Novem Mestu	Fakulteta za Informacijske Študije	Informatika v sodobni družbi	Mag	Varnost elektronskega poslovanja	Obvezni
Fakulteta za Komercialne in Poslovne Vede	/	Poslovna informatika I	VS	Varnost informacijskih sistemov	Obvezni
Fakulteta za Komercialne in Poslovne Vede	/	Poslovna informatika II	Mag	Varnostne tehnologije v IS	Izbirni
Fakulteta za Komercialne in Poslovne Vede	/	Varnostni menedžment	Mag	Kibernetska varnost	Obvezni
Fakulteta za Komercialne in Poslovne Vede	/	Varnostni menedžment	Mag	Varnostne tehnologije v IS	Izbirni
Fakulteta za Medije	/	Mediji in novinarstvo Strateško komuniciranje	Mag	Varno spletno komuniciranje	Izbirni
Gea College	/	Podjetniški management Upravljanje s tveganji in korporativna varnost	Mag	Business Intelligence in varovanje poslovnih informacij Informacijska varnost in neprekinjeno poslovanje	Izbirni
Mednarodna podiplomska šola Jožefa Stefana	/	Informacijske in komunikacijske tehnologije	Mag	Informacijska varnost in ekonomija tveganj	Izbirni
Mednarodna podiplomska šola Jožefa Stefana	/	Informacijske in komunikacijske tehnologije	Mag	Varnost informacijskih sistemov	Izbirni
Mednarodna podiplomska šola Jožefa Stefana	/	Informacijske in komunikacijske tehnologije	Mag	Digitalna forenzika	Izbirni
Mednarodna podiplomska šola Jožefa Stefana	/	Informacijske in komunikacijske tehnologije	Mag	Digitalna forenzika II	Izbirni
Mednarodna podiplomska šola Jožefa Stefana	/	Informacijske in komunikacijske tehnologije	Dr	Varnost v internetnih tehnologijah	Izbirni
Fakulteta za management in pravo	/	Management in poslovno pravo	Mag	Informacijska varnost	Izbirni
Univerza na Primorskem	Fakulteta za matematiko, naravoslovje in informacijske tehnologije	Matematika	UN	Kriptografija in računalniška varnost	Izbirni
Univerza v Ljubljani	Fakulteta za Elektrotehniko	Elektrotehnika - Informacijsko komunikacijske tehnologije	Mag	Varnost informacijsko komunikacijskih sistemov	Obvezni
Univerza v Ljubljani	Fakulteta za Elektrotehniko	Multimedija	UN	Varnost komunikacij in zaščita vsebin	Obvezni
Univerza v Ljubljani	Fakulteta za računalništvo in informatiko	Računalništvo in informatika	VS	Komunikacijski protokoli in omrežna varnost	Obvezni

Univerza v Ljubljani	Fakulteta za računalništvo in informatiko	Računalništvo in informatika Multimedija Računalništvo in informatika	Mag	Kriptografija in računalniška varnost	Obvezni
Univerza v Ljubljani	Fakulteta za računalništvo in informatiko	Računalništvo in informatika Multimedija Računalništvo in matematika Pedagoško računalništvo in informatika	Mag	Informacijska varnost in zasebnost	Izbirni
Univerza v Mariboru	Fakulteta za elektrotehniko, računalništvo in informatiko	Telekomunikacije	Mag	Varovanje omrežnih naprav	Izbirni
Univerza v Mariboru	Fakulteta za elektrotehniko, računalništvo in informatiko	Medijske komunikacije	Dr	Uporabniški vidiki informacijske varnosti	Izbirni
Univerza v Mariboru	Fakulteta za elektrotehniko, računalništvo in informatiko	Računalništvo in informatika	Dr	Informacijska zasebnost in varnost	Izbirni
Univerza v Mariboru	Fakulteta za elektrotehniko, računalništvo in informatiko	Informatika in tehnologije komuniciranja Računalništvo in informacijske tehnologije	VS	Varnost in zaščita	Obvezni
Univerza v Mariboru	Fakulteta za elektrotehniko, računalništvo in informatiko	Informatika in tehnologije komuniciranja	UN	Osnove informacijske varnosti	Obvezni
Univerza v Mariboru	Fakulteta za organizacijske vede	Organizacija in management poslovnih in delovnih sistemov Organizacija in management informacijskih sistemov Organizacija in management kadrovskih in izobraževalnih sistemov	Dr	Zanesljivosti, razpoložljivosti in varnost informacijskih sistemov	Izbirni
Univerza v Mariboru	Fakulteta za organizacijske vede	Organizacija in management informacijskih sistemov	VS	Uvod v informacijsko varnost	Obvezni
Univerza v Mariboru	Fakulteta za organizacijske vede	Organizacija in management informacijskih sistemov	UN	Informacijska varnost	Obvezni
Univerza v Mariboru	Fakulteta za organizacijske vede	Organizacija in management informacijskih sistemov	Mag	Kibernetska varnost	Izbirni
Univerza v Novem Mestu	Fakulteta za ekonomijo in informatiko	Poslovna informatika Računalništvo in informatika	VS	Varnostne politike	Obvezni
Univerza v Novem Mestu	Fakulteta za ekonomijo in informatiko	Računalništvo in informatika	VS	Varnost računalniških sistemov	Obvezni
Univerza v Novi Gorici	Poslovno-tehniška fakulteta	Gospodarski inženiring	VS	Informacijska varnost	Izbirni