

UČNI NAČRT PREDMETA / COURSE SYLLABUS

Predmet: Presoja in revidiranje kibernetске varnosti
Course title: Assessment and audit of cyber security

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester Semester
Kibernetска varnost, magistrski študijski program druge stopnje	-	Drugi	Tretji
The second cycle masters study programme Cyber Security	-	Second	Third

Vrsta predmeta / Course type

Obvezni / Obligatory

Univerzitetna koda predmeta / University course code:

5-KV-MAG-PRKV-2026-01-21

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
25	-	12	-	-	83	4

Nosilec predmeta / Lecturer: doc. dr. Boštjan Delak

Jeziki / Languages:

Predavanja / Lectures: Slovenski, angleški / Slovene, English

Vaje / Tutorial: Slovenski, angleški / Slovene, English

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:

Za vključitev v delo je potrebno usvojiti zanje predmetov iz 1. letnika študija.

Pomembno je poznavanje:

- Osnov informacijske varnosti
- Osnove upravljanja IS
- Poznavanje komponent IS
- Varnega in zanesljivega delovanja IS
- Varnega razvoja programske opreme
- Upravljanje in ocenjevanje tveganj

Študent/študentka mora pred pristopom k izpitu pripraviti in zagovarjati seminarsko nalogo.

Prerequisites:

In order to be included in the work, it is necessary to master the content of the courses from the 1st year study.

It is important to know:

- Basics of information security
- Basics of IS management
- Knowledge of IS components
- Safe secure and reliable IS operation
- Safe and secure software development
- Risk management and assessment

Prior to the exam, the student has to prepare and present seminar work.

Vsebina:

Content (Syllabus outline):

- Presoje kiberentske varnosti: pristop, ocena tveganja, standardi, načrt presoje, izvedba, poročanje
- Revidiranje kibernetike varnosti: ocena tveganj, določitev namena in ciljev, uporabljena sodila (metodologije, okvirji, smernice, dobre prakse), načrt revizije, izvedba, izdelava revizijskega poročila, poročanje, oirevizijski pregled.
- Penetracijski testi: Tipi, pristop, izvedba, poročila.

- Cyber security assessments: approach, risk assessment, standards, assesment plan, realization, reporting
- Cyber security auditing: risk assessment, determination of purpose and objectives, applied criteria (methodologies, frameworks, guidelines, best practices), audit plan, audit realization, preparation of audit report, reporting, audit review.
- Penetration tests:
- Types, approach, implementation, reports.

Temeljni literatura in viri / Readings:

- T. Schneider, *Cybersecurity Law, Standards and Regulations: 2nd Edition*, Rothstein Publishing, 2020 (Izbrana poglavja).
- Y. Diogenes, E. Ozkaya, *Cybersecurity – Attack and Defense Strategies*, Packt Publishing, 2018 (Izbrana poglavja).
- D. Death, *Information Security Handbook, 2nd Edition*, Packt Publishing, 2023 (Izbrana poglavja).
- ENISA, *Methodology for a Sectoral Cybersecurity Assessment*, ENISA, 2021,
- W. Chuck, *Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits*, Pearson, 2018 (Izbrana poglavja).
- J. Rehberger, *Cybersecurity Attacks – Red Team Strategies*, Packt, 2020.
- J. J. Champlain, *Auditing Information Systems*, Wiley, 2003 (Izbrana poglavja).
- S. Snft, F. Gallegos, A. Davis, *Information Technology Control and Audit*, CRC Press, 2013 (4. izdaja) (Izbrana poglavja).

Cilji in kompetence:

Učna enota prispeva k razvoju naslednjih splošnih in predmetno specifičnih kompetenc:

Splošne kompetence:

- razumevanje pomena kibernetike varnosti,
- sposobnost identifikacije kibernetičnih varnostnih tveganj ter izdelave predlogov za ukrepanje in zaščito na osnovi identificiranih tveganj,
- sposobnost uporabe različnih programskih rešitev za zagotavljanje, upravljanje, nadzorovanje in evalvacijo kibernetike varnosti,
- sposobnost iskanja podatkov in virov za potrebe upravljanja kibernetike varnosti,

Predmetno-specifične kompetence:

Objectives and competences:

The instructional unit contributes to the development of the following general and subject-specific competences:

General competences:

- understanding the importance of cyber security,
- the ability to identify cyber security risks and make proposals for action and protection based on identified risks,
- the ability to use various software solutions to provide, manage, monitor and evaluate cyber security
- the ability to find data and sources for the needs of cyber security management,

Subject-specific competences:

- sposobnost načrtovanja in naročanje revizijskega pregleda kibernetske varnosti ali njenih komponent,
- sposobnost načrtovanja in naročanja presoj kibernetske varnosti,
- sposobnost načrtovanja in naročanja različnih oblik penetracijskih testov;

- the ability to plan and commission an audit of cyber security or its components,
- the ability to plan and commission cyber security assessments,
- the ability to plan and order various forms of penetration tests;

Predvideni študijski rezultati:

Znanje in razumevanje:

Sposobnost študenta/študentke bo:

- načrtovanje, izvedba in uspešen zaključek projektov testiranja, evalvacije in revidiranja kibernetske varnosti
- poznavanje tehnik in orodij, potrebnih za izvajanje opravil testiranja, evalvacije in revizije
- uspešno sodelovanje z internim in zunanjim revizorjem informacijskih sistemov in kibernetskimi veščaki

Intended learning outcomes:

Knowledge and understanding:

The ability of the students will be:

- planning, execution and successful completion of testing, evaluation and auditing of cybersecurity
- knowledge of techniques and tools necessary to perform tasks of testing, evaluation and audit
- successful cooperation with internal and external information systems auditors and cyber specialists

Metode poučevanja in učenja:

- *predavanja z aktivno udeležbo študentov (razlaga, diskusija, vprašanja, primeri, reševanje problemov)*
- *vaje z izdelavo domačih nalog in izdelava seminarske naloge*
- *individualne in skupinske konzultacije (diskusija, dodatna razlaga, obravnava specifičnih vprašanj)*

Learning and teaching methods:

- *lectures with active participation of students (explanation, discussion, questions, examples, problem solving)*
- *exercises with homeworks and seminar work*
- *individual and group consultations (discussion, additional explanation deals with specific issues)*

Delež (v %) /

Weight (in %)

Načini ocenjevanja:

Assessment:

Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
<ul style="list-style-type: none"> • pisni izpit • zagovor seminarske naloge • domače naloge 	<p>60</p> <p>24</p> <p>16</p>	<ul style="list-style-type: none"> • written exam • preparation and presentation of seminar work • homework

Reference nosilca / Lecturer's references:

- DREV, Matjaž, DELAK, Boštjan. Automating privacy compliance. V: ERMAN, Nuša (ur.). 14th International Conference on Information Technologies and Information Society: ITIS 2023: ["Future of digital society in the age of AI and ChatGPT"]: conference proceedings: November 9-10, 2023, Ljubljana, Slovenia. Novo mesto: Faculty of Information Studies, 2024. Str. 139-144.

- DELAK, Boštjan, KRANJEC, Miroslav. Performing a Cybersecurity Audit of an Electric Power Transmission Systems Operator, ISACA Journal, 2023, vol. 1, str. 46-52.
- DREV, Matjaž, DELAK, Boštjan. Conceptual Model of Privacy by Design. *Journal of computer information systems*. 2022, vol. 62, iss. 5, str. 888-895.
- DELAK, Boštjan. Revizija neprekinjenega poslovanja = Business continuity audit. *Sir*ius: revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij*. 2019, št. 5, str. 3-17. ISSN 2335-3252. <http://www.si-revizija.si/publikacijesirius/kazala-letnikov>. [COBISS.SI-ID 2048620563].
- DAVIS, Keiona, LEVY, Yair, DELAK, Boštjan. Towards a development of cybersecurity risk-responsibility taxonomy of small enterprises for data breach mitigation. V: *Digital disruption. 24th Americas Conference on Information Systems (AMCIS)*, New Orleans, LA, August 16-18, 2018. [S. l.]: Association for Information Systems, 2018. Str. 1-6. ISBN 978-0-9966831-6-6-
<https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1338&context=amcis2018>,
<https://aisel.aisnet.org/amcis2018/Security/Presentations/8/>. [COBISS.SI-ID 2048569363].
- DELAK, Boštjan. Revizija stanja kibernetike varnosti = Cybersecurity auditing. *Sir*ius: revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij*. 2017, št. 5, str. 25-51. ISSN 2335-3252, <http://www.si-revizija.si/publikacijesirius/kazala-letnikov>. [COBISS.SI-ID 2048476179].
- DELAK, Boštjan. Izzivi revizorjev informacijskih sistemov pri dajanju zagotovil pri logičnih dostopih = The information systems auditors' issues at the logical access audit assurance activities. *Sir*ius: revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij*. sep. 2016, let. 4, št. 5, str. 5-27, graf. prikazi, tabele. ISSN 2335-3252. [COBISS.SI-ID 23241958].
- DELAK, Boštjan. Revizijska sled v informacijskih sistemih v teoriji in praksi = Information System Audit Trail in Theory and Praxis. *Sir*ius: revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij*. 2014, št. 5, str. 5-27. ISSN 2335-3252. [COBISS.SI-ID 2048332051].
- DELAK, Boštjan, BAJEC, Marko. Framework for the delivery of information system due diligence. *Information systems management*, ISSN 1058-0530, 2013, vol. 30, no. 1, str. 137-149.
- DELAK, Boštjan, BAJEC, Marko. Conducting IS due diligence in a structured model within a short period of time. *ISACA journal*, ISSN 1944-1975, 2014, vol. 4, str. 1-6.