UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Varnost sistemov
Course title:	Systems Security

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester Semester
Kibernetska varnost, magistrski študijski program druge stopnje	-	Prvi	Prvi
Cyber Security, second cycle Masters Study Programme	-	First	First

Vrsta predmeta / Course type | Obvezni / Obligatory

Univerzitetna koda predmeta / University course code: | 5-KV-MAG-VS-2021-12-14

Predavanja Lectures	Seminar Seminar	Vaje Tutorial	Klinične vaje work	Druge oblike študija	Samost. delo Individ. work	ECTS
30	/	45	/	/	105	6

Nosilec predmeta / Lecturer: | izr. prof. dr. Blaž Rodič

Jeziki / Languages:	Predavanja / Lectures:	slovenski / Slovenian, angleški / English
	Vaje / Tutorial:	slovenski / Slovenian, angleški / English

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

Študent/študentka mora pred pristopom k izpitu imeti pozitivno ocenjene vaje in seminarsko nalogo.

Prerequisits:

Positively evaluated exercises and seminar paper are prerequisites for exam.

Vsebina:

- Uvod v predmet:
  Namen študija predmeta, povezanost predmeta z drugimi predmeti, vsebina študija predmeta, študijska literatura.
- Teorija sistemov, sistemski pristop/holistični pristop k obravnavi sistemov, sistemski inženiring
- Informacijski sistemi (IS), namen in cilji informacijskega sistema, klasifikacija informacijskih sistemov
- Življenjski cikel razvoja informacijskih sistemov
- Temelji varnosti IS, Koncept varnosti z zasnovo

Content (Syllabus outline):

- Introduction**:**
  The purpose of the subject, connections with other subjects, subject contents, study literature.
- Systems theory, systemic approach/holistic approach to systems, system engineering
- Information Systems, Purpose and goals of IS, Information systems classification.
- Information System Development Life Cycle
- Information system security fundamentals, The Security by Design concept

• Modeliranje varnosti IS: Ranljivosti, grožnje, tveganja, in ukrepi/kontrole na področju varnosti sistemov • Sistemsko upravljanje: Sistemi in postopki, Dokumentacija, Modeli politik, Sestava politike, Varnostni popravki in življenjski cikel ranljivosti, Delovanje sistema, Zagon in razgradnja sistema, notranje grožnje • Nadzor dostopa: metode avtentikacije, identiteta • Sistemski nadzor: nadzor dostopa, avtorizacijski modeli, zaznavanje vdorov, napadi, obramba, revizija, modeli ranljivosti, penetracijsko testiranje, forenzika • Ukinitev sistema: razgradnja, odstranjevanje sistema • Preizkušanje sistemov: preverjanje zahtev, preverjanje sestave komponent, testiranje enot v primerjavi s testiranjem sistema, formalno preizkušanje sistemov • Pogoste sistemske arhitekture: virtualni strežniki, industrijski nadzorni sistemi, internet stvari (IoT), vgrajeni sistemi, mobilni sistemi, avtonomni sistemi, sistemi splošnega namena • Varnostni modeli, primeri varnih sistemskih arhitektur • Vloga mednarodnih standardov informacijske varnosti v procesu zagotavljanja varnosti sistemov	• IS security modelling: System Vulnerabilities, Threats, Risks and Countermeasures • System Management: Systems and procedures, Documentation, Policy models, Policy composition, Patching and the vulnerability life cycle, System Operation, Commissioning and Decommissioning, Insider threats • System Access: Authentication methods, Identity • System control: Access control, Authorization models, Intrusion detection, Attacks, Defenses, Auditing, Vulnerabilities models, Penetration testing, Forensics • System Retirement: Decommissioning, Disposal • System Testing: Validating requirements, Validating composition of components, Unit versus system testing, Formal verification of systems • Common System Architectures: Virtual machines, Industrial control systems, Internet of Things (IoT), Embedded systems, Mobile systems, Autonomous systems, General-purpose systems • Security models, Secure System Architecture examples • Role of ITSEC standards in systems security

Temeljni literatura in viri / Readings:

- Moyle, E., Kelly, D., (2020) Practical Cybersecurity Architecture, Packt Publishing.
- Melone, M., (2021), Designing Secure Systems, CRC Press.

Izbrana poglavja iz:
- Bavec, C., Kovačič, A., Krisper, M. ,Rajkovič, V. and Vintar, M., (2019) Slovenija na poti digitalne preobrazbe. Založba UL FRI, Ljubljana, Ljubljana. ISBN 978-961-7059-01-4
- Blum, D., (2020) Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment, Springer.
- Knapp, E. D. and Langill, J. T. (2015) Industrial Network Security. 2nd edn, Industrial Network Security. 2nd edn. Elsevier. doi: 10.1016/c2013-0-06836-3.

Cilji in kompetence:	**Objectives and competences:**

Cilj predmeta je študentom omogočiti celosten pogled na sisteme z varnostnega vidika in znanje o varnostnih vidikih sistemov, ki so sestavljeni iz komponent in povezav in katerih del je programska oprema. Študentje preučijo varnostno problematiko povezovanja komponent in njihove uporabe v večjih sistemih.

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

Splošne kompetence:
- Razumevanje pomena kibernetske varnosti;
- Sposobnost pridobivanja, selekcije, analize informacij in zmožnost njihove interpretacije za celovito reševanje problemov, izzivov in incidentov s področja kibernetske varnosti.
- Poznavanje uveljavljenih metodoloških pristopov za upravljanje varnosti sodobnih informacijskih sistemov in omrežij.

Predmetno-specifične kompetence:
- Sposobnost uporabe holističnega, sistemskega pristopa pri obravnavanju varnosti informacijskih sistemov;
- Sposobnost razumevanja in priprave varnostnih politik informacijskih sistemov;
- Sposobnost razvoja in testiranja sistemov za nadzor dostopa;
- Poznavanje sistemov za detekcijo poskusov vdora, penetracijsko testiranje in postopkov ob zaznavi poskusa vdora v sistem;
- Poznavanje postopkov za zagotavljanje neprekinjenega poslovanja;
- Obvladovanje postopkov dokumentiranja vzpostavitve, obratovanja in ukinitve sistema.

Goal of the course is to provide students with a holistic view on systems from security aspect and with knowledge on security aspects of software enabled systems, which are composed of components and connections. Students are to study security issues of connecting components and using them within larger systems.

Course contributes to the development of the following general and subject-specific competences:

General competences:
- Understanding the importance of cyber security;
- The ability to obtain, select, analyze information, as well as to interpret them to comprehensively solve problems, challenges and incidents in the field of cyber security;
- Knowledge of established methodological approaches for security management of modern information systems and networks.

Subject-specific competences:
- Ability to use a holistic, systemic approach in addressing the security of information systems;
- Ability to understand and prepare information system security policies;
- Ability to develop and test access control systems;
- Knowledge of intrusion detection detection systems, penetration testing and intrusion detection detection procedures;
- Knowledge of procedures for ensuring business continuity;
- Mastering the procedures for documenting the establishment, operation and decommissioning of the system.

Predvideni študijski rezultati:

Znanje in razumevanje:

Študent/študentka je sposoben:

Intended learning outcomes:

Knowledge and understanding:

The student can:

- razumeti koncepte sistemske teorije in sistemskega/celostnega pristopa; - pojasniti, kaj je varnostna politika in njeno vlogo pri zaščiti podatkov in virov; - pojasniti tri lastnosti, ki se običajno uporabljajo za preverjanje pristnosti; - opisati fizični in logični nadzor dostopa ter ju primerjati; - razpravljati o tem, kako sistemi za odkrivanje vdorov prispevajo k varnosti; - razložiti, kaj je odpornost, in opredeliti okolje, v katerem je pomembna; - opisati, kaj je penetracijski test in zakaj je pomemben; - razpravljati o pomenu dokumentiranja pravilne namestitve in konfiguracije sistema.	- understand the concepts of systems theory and system/holistic approach; - explain what a security policy is, and its role in protecting data and resources; - explain three properties commonly used for authentication; - describe physical and logical access control, and compare them; - discuss how intrusion detection systems contribute to security; - explain what resilience is and identify an environment in which it is important; - describe what a penetration test is and why it is valuable; - discuss the importance of documenting proper installation and configuration of a system.

Metode poučevanja in učenja:

Learning and teaching methods:

Predavanja z aktivno udeležbo študentov; *Laboratorijske vaje*; *Individualno delo*; študij znanstvene in strokovne literature in priprava empirične seminarske naloge.	*Lectures* with the active participation of students; *Laboratory exercises*; *Individual work*: study of scientific and professional literature and development of empirical seminar work

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
- pisni izpit - empirična seminarska naloga, poročila laboratorijskih vaj	50 50	- written exam - empirical seminar work, report on laboratory exercises

Reference nosilca / Lecturer's references:

- RODIČ, Blaž. Industry 4.0 and the new simulation modelling paradigm. Organizacija : revija za management, informatiko in kadre, ISSN 1318-5454. [Tiskana izd.], aug. 2017, vol. 50, no. 3, str. 193-207, ilustr., doi: 10.1515/orga-2017-0017
- BRELIH, Marjan, RAJKOVIČ, Uroš, RUŽIČ, Tomaž, RODIČ, Blaž, KOZELJ, Daniel. Modelling decision knowledge for the evaluation of water management investment projects. Central European Journal of Operations Research, ISSN 1435-246X, 2018, vol. , iss. , str. https://link.springer.com/content/pdf/10.1007%2Fs10100-018-0600-5.pdf, doi: 10.1007/s10100-018-0600-5.
- KANDUČ, Tadej, RODIČ, Blaž. Optimisation of machine layout using a force generated graph algorithm and simulated annealing. International journal of simulation modelling, ISSN 1726-4529, 2016, vol. 15, no. 2, str. 275-287.

- RODIČ, Blaž, BAGGIA, Alenka. Dynamic airport ground crew scheduling using a heuristic scheduling algorithm. International journal of applied mathematics and informatics, ISSN 2074-1278, 2013, vol. 7, iss. 4, str. 153-163.
- RODIČ, Blaž. Mobile agents for distributed decision support systems. The International Scientific Journal of Management Information Systems, ISSN 1452-774X, 2011, vol. 6, no. 1, str. 20-27.
- RODIČ, Blaž, KLJAJIĆ, Miroljub. Accessing distributed data sources with mobile agents and XML. V: JAŠKOVÁ, Mária (ur.). ECON '05 : [selected research papers], (Research works proceedings, ISSN 0862-7908, Vol. 12, 2005). Ostrava: Technical University of Ostrava, Faculty of Economics. 2005, str. 280-287.
- RODIČ, Blaž, KLJAJIĆ, Miroljub. Integracija simulacijskih orodij v e-poslovni informacijski sistem. V: GRIČAR, Jože (ur.). Izboljšanje konkurenčnosti regije z e-poslovanjem, (Organizacija, ISSN 1318-5454, Letn. 37, 2004, št. 3). Kranj: Moderna organizacija. 2004, str. 162-167.
- ŠKRABA, Andrej, BAGGIA, Alenka, RODIČ, Blaž. Application of a group decision support system in the reform of study programmes. V: DONDON, Philippe (ur.). Recent advances in education and modern educational technologies, (Educational technologies series, 9). [S. l.: s. n.]. 2013, str. 128-134.
- RODIČ, Blaž. Issues of e-collaboration and knowledge management in media industries. V: LUGMAYR, Artur (ur.), et al. Information systems and management in media and entertainment industries, (International series on computer entertainment and media technology (Online), ISSN 2364-9488). Cham: Springer. cop. 2016.