UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Razvoj varne programske opreme
Course title:	Secure Software Development

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

Vrsta predmeta / Course type	Obvezni / Obligatory
Univerzitetna koda predmeta / University course code:	5-KV-MAG-RVPO-2021-12-14

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
30	/	30	/	/	120	6

Nosilec predmeta / Lecturer:	Izr. prof. dr. Borut Lužar

Jeziki /	**Predavanja / Lectures:**	Slovenski / Angleški
Languages:	**Vaje / Tutorial:**	Slovenski / Angleški

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

Za vključitev v delo je potrebno osnovno znanje enega izmed splošnih programskih jezikov in usvojeno zanje predmetov Pravo informacijske varnosti in Varnost sistemov.

To enroll into this class, basic knowledge of one of common programming languages is required, and to master the content of the Information Security Law and System security courses.

Vsebina:

- Življenjski cikel razvoja programske opreme
- Zlonamerna in napačna uporaba programske opreme
- Ocena varnostnih tveganj
- Načrtovalski vzorci
- Načrtovanje testov
- Modeliranje groženj
- Obrambno kodiranje
- Pregled kode
- Dovoljenja za dostope (uporabniki, datoteke …)
- Kriptografski algoritmi
- Umestitev programske opreme v produkcijsko okolje
- Notranje grožnje (s strani zaposlenih in drugih deležnikov)
- DevOps paradigma in orodja

Content (Syllabus outline):

- Lifecycle of software development
- Cases of software abuse and misuse
- Security risk assessment
- Design patterns
- Test planning
- Threat modeling
- Defensive coding
- Code inspection
- Access permissions (users, files …)
- Cryptographic algorithms
- Production deployment
- Insider threats (by employees and other entrepreneurs)
- DevOps paradigm and tools

Temeljni literatura in viri / Readings:

- Prosojnice in zapiski predavanj pri predmetu
- Howard, M., Lipner, S. (2006). The Security Development Lifecycle Book, Microsoft Press, ZDA.
- Klein, B. T. (2021). The DevOps: A Concise Understanding to the DevOps Philosophy and Science. Technical Report.
- Kohnfender, L. (2021). Designing Secure Software: A guide for developers, No Starch Press.
- Payer, M., Rashild, A., Such, J. M. (editors, 2018). Engineering Secure Software and Systems, in Lecture Notes in Computer Science, Springer, Cham, Germany.
- Richardson, T., Thies, C. N. (2012). Secure Software Design, Jones and Bartlett Learning, MA, ZDA.

Cilji in kompetence:

Objectives and competences:

Splošne kompetence: • Sposobnost identifikacije kibernetskih varnostnih tveganj ter izdelave predlogov za ukrepanje in zaščito na osnovi identificiranih tveganj. • Sposobnost uporabe različnih programskih rešitev za zagotavljanje, upravljanje, nadzorovanje in evalvacijo kibernetske varnosti. • Sposobnost iskanja podatkov in virov za potrebe upravljanja kibernetske varnosti. • Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetski varnosti v praksi.	***General competences:*** • 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. • The ability of flexible usage of the acquired knowledge on cyber security in practice.
Predmetno-specifične kompetence: • zavedanje varnostnih groženj pri razvoju programske opreme, • sposobnost kritično oceniti in izbrati tehnologije, ki podpirajo varnost programske opreme, • sposobnost kritično analizirati razvoj programske opreme in svetovali, kako se lahko izboljša z varnostnega vidika, • sposobnost kritično ovrednotiti varnost razvite programske opreme.	***Subject-specific competences:*** • awareness of software development security threats; • ability to critically assess and choose technologies supporting software security; • ability to critically analyze software development and suggest security improvements; • ability to critically asses security of already developed software.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Znanje in razumevanje: • usposobljenost za prepoznavanje varnostnih groženj v programski opremi, • razumevanje procesa razvoja varne programske opreme, • poznavanje orodij in pristopov k razvoju varne programske opreme,	Knowledge and understanding: • ability to recognize security threats in software; • understanding of secure software development process; • knowledge and understanding of tools and principles used for secure software development.

Metode poučevanja in učenja:	**Learning and teaching methods:**
• *Predavanja z aktivno udeležbo študentov* (razlaga, diskusija, vprašanja, primeri, reševanje problemov);	• *Lectures with active participations by the students* (explanation, discussion, questions, cases, problems solving);

- *Vaje*, kjer študentje na primerih ponovijo temeljne koncepte, predstavljene na predavanjih;	- *Tutorials*, where students will recall, reinforce, and shed light on the concepts and methods introduced at lectures;

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt): Pisni izpit	100 %	Type (examination, oral, coursework, project): Written Exam

Reference nosilca / Lecturer's references:

- P. Holub, B. Lužar, E. Mihaliková, M. Mockovčiaková, R. Soták: Star edge-coloring of square grids, Appl. Math. Comput. 392 (2021), 125741.
- K. Rojko, B. Bratić, B. Lužar: The Bologna reform's impacts on the scientific publication performance of Ph.D. graduates - the case of Slovenia, Scientometrics 124 (2020), 329-356.
- M. Šurimová, B. Lužar, T. Madaras: Adynamic coloring of graphs, Discrete Appl. Math. 284 (2020), 224-233.
- B. Lužar, M. Mockovčiaková, P. Ochem, A. Pinlou, R. Soták: On non-repetitive sequences of arithmetic progressions: the cases k ∈ {4,5,6,7,8}, Discrete Appl. Math. 279 (2020), 106-117.
- F. Dross, B. Lužar, M. Maceková, R. Soták: Note on 3-choosability of planar graphs with maximum degree 4, Discrete Math. 342(11) (2019), 3123-3129.
- B. Lužar, M. Mockovčiaková, R. Soták: Note on list star edge-coloring of subcubic graphs, J. Graph Theory 90(3) (2019), 304-310.
- A. Kastrin, J. Klisara, B. Lužar, J. Povh: Is science driven by principal investigators?, Scientometrics 117(2) (2018), 1157-1182.
- B. Lužar, J. Przybyło, R. Soták: New bounds for locally irregular chromatic index of bipartite and subcubic graphs, J. Combin. Optim. 36(4) (2018), 1425-1438.
- B. Lužar, P. Ochem, A. Pinlou: On repetition thresholds of caterpillars and trees of bounded degree, Electron J. Combin. 25 (2018), #P1.61.
- V. Andova, B. Lidický, B. Lužar, R. Škrekovski: On facial unique-maximum (edge-)coloring, Discrete Appl. Math. 237 (2018), 26-32.
- B. Lužar, M. Petruševski, R. Škrekovski: On vertex-parity edge-colorings, J. Combin. Optim. 35 (2018), 373-388.