1.	**Course title**	Security incident and response management
2.	**Course code**	ИТ-И-16
3.	**Semester**	9
4.	**Unit offering the course**	Faculty of Computer Science and Engineering
5.	**ECTS**	6
6.	**Goals of the study programme**	
	The goals of the course is to enable the students to gain knowledge about incident management connected to system security. The student will be able to differentiate between events and incidents and classify incidents. The students will know how to develop an incident response policy and will be able to explore network and host based artefacts in order to determine the root cause. The student will have knowledge about the tools and support packets used in the area.	
7.	**Contents of the study programme**	
	Design, building, operations and development of a Computer Emergency Response Team (CERT). Managing a Security operations centre. Incident response, incident response plan. Security events management. Vulnerability assessment, incident analysis. Policy requirements. Laws and policies in use. Containment. Forensics and research, Evidence handling. Forensics team operations. Forensics laws. Managing and communicating the information. Teams relationship.	