The list of topics for M.Sc. diploma examination – COMPUTING Specialization:

Cybersecurity

Remark! Learning objectives that are not present in the column *Symbols of learning objective being verified* are verified during the admission process.

	Topic	Symbols of learning objective being verified
1.	Threats and vulnerabilities in wireless communication systems.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2
2.	Jamming – general description, modes, applications.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2
3.	DoS attacks in wireless networks.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2
4.	WPA3 protection.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2
5.	IEEE 802.11 evolution of protection methods.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2
6.	Safety integrity levels (SIL): definition, principles of use.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
7.	Faults, errors, and failures: definitions, impact on the system.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
8.	Safety instrumented functions (SIF) and safety instrumented system (SIS).	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
9.	Usage of SIS and SIF of critical systems.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
10.	Voting mechanisms. Symbols and principle of functioning.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
11.	Tools for assessing the threat and the safety integrity levels.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
12.	Types of redundancy in critical systems.	K2st_U1, K2st_U3, K2st_U4, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
13.	Basic elements of software-defined networks SDN.	K2st_U1, K2st_U3, K2st_U5, K2st_U8, K2st_U12, K2st_U15, K2st_U16 K2st_K1, K2st_K2

14.	The concept of mobile target defense MTD.	K2st_U1, K2st_U3, K2st_U5, K2st_U8, K2st_U12, K2st_U15, K2st_U16 K2st_K1, K2st_K2
15.	Vulnerabilities, threats, attacks, risks.	K2st_U1, K2st_U3, K2st_U6, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
16.	Planes of cybersecurity cube.	K2st_U1, K2st_U3, K2st_U6, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
17.	Common access control models.	K2st_U1, K2st_U3, K2st_U6, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
18.	Reconnaissance Attacks.	K2st_U1, K2st_U3, K2st_U6, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
19.	Network Taps and SPANs.	K2st_U1, K2st_U3, K2st_U6, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
20.	SOC metrics.	K2st_U1, K2st_U3, K2st_U6, K2st_U8, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K4
21.	OWASP TOP10, Broken Access Control, Cryptographic Failures - sample scenario and methods to protect against these threats.	K2st_U1, K2st_U2, K2st_U3, K2st_U4, K2st_U5, K2st_U6 K2st_K1, K2st_K2, K2st_K4
22.	OWASP TOP10, Injection, Insecure Design, sample scenario and methods to protect against these threats.	K2st_U1, K2st_U2, K2st_U3, K2st_U4, K2st_U5, K2st_U6 K2st_K1, K2st_K2, K2st_K4
23.	OWASP TOP10, Identification and Authentication Failures, Software and Data Integrity Failures, sample scenario and methods to protect against these threats.	K2st_U1, K2st_U2, K2st_U3, K2st_U4, K2st_U5, K2st_U6 K2st_K1, K2st_K2, K2st_K4
24.	OWASP TOP10, Security Logging and Monitoring Failures, Server-Side Request Forgery, sample scenario and methods to protect against these threats.	K2st_U1, K2st_U2, K2st_U3, K2st_U4, K2st_U5, K2st_U6 K2st_K1, K2st_K2, K2st_K4
25.	Authentication methods in web applications using cookies, JWT, OAuth, OpenID.	K2st_U1, K2st_U2, K2st_U3, K2st_U4, K2st_U5, K2st_U6 K2st_K1, K2st_K2, K2st_K4
26.	Application testing methods.	K2st_U1, K2st_U2, K2st_U3, K2st_U4, K2st_U5, K2st_U6 K2st_K1, K2st_K2, K2st_K4
27.	Classifications of threats in risk analysis of IT systems.	K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U11, K2st_U13, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K3, K2st_K4

28.	Risk analysis methods: quantitative, qualitative, semiquantitative.	K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U11, K2st_U13, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K3, K2st_K4
29.	Treats modelling, STRIDE.	K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U11, K2st_U13, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K3, K2st_K4
30.	Penetration tests.	K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U11, K2st_U13, K2st_U15, K2st_U16 K2st_K1, K2st_K2, K2st_K3, K2st_K4
31.	Confusion and diffusion proposed by Shannon – what does it mean and which components of block cipher are responsible for this.	K2st_W2, K2st_W3, K2st_W4, K2st_W6 K2st_U1, K2st_U3, K2st_U4, K2st_U5, K2st_U7, K2st_U11, K2st_U16 K2st_K1, K2st_K2, K2st_K3
32.	Modes of operations, security considerations: which should be used?	K2st_W2, K2st_W3, K2st_W4, K2st_W6 K2st_U1, K2st_U3, K2st_U4, K2st_U5, K2st_U7, K2st_U11, K2st_U16 K2st_K1, K2st_K2, K2st_K3
33.	Security properties of an S-box.	K2st_W2, K2st_W3, K2st_W4, K2st_W6 K2st_U1, K2st_U3, K2st_U4, K2st_U5, K2st_U7, K2st_U11, K2st_U16 K2st_K1, K2st_K2, K2st_K3
34.	Hash functions: properties, constructions, where are they used.	K2st_W2, K2st_W3, K2st_W4, K2st_W6 K2st_U1, K2st_U3, K2st_U4, K2st_U5, K2st_U7, K2st_U11, K2st_U16 K2st_K1, K2st_K2, K2st_K3
35.	Authenticated Encryption algorithms.	K2st_W2, K2st_W3, K2st_W4, K2st_W6 K2st_U1, K2st_U3, K2st_U4, K2st_U5, K2st_U7, K2st_U11, K2st_U16 K2st_K1, K2st_K2, K2st_K3
36.	Characteristics of the digital forensics process.	K2st_U1, U2st_U6, K2st_U8, K2st_U9, K2st_U12, K2st_U16 K2st_K1, K2st_K2, K2st_K3, K2st_K4
37.	ENISA Threat Landscape, Characteristics of the most important cyber threats.	K2st_U1, U2st_U6, K2st_U8, K2st_U9, K2st_U12, K2st_U16

		K2st_K1, K2st_K2, K2st_K3, K2st_K4
38.	OSINT - characteristics of open-source data, the investigation process and the main advantages and risks.	K2st_U1, U2st_U6, K2st_U8, K2st_U9, K2st_U12, K2st_U16 K2st_K1, K2st_K2, K2st_K3, K2st_K4
39.	Classifications of malware: categories, similarities, and differences.	K2st_U1, K2st_U3, K2st_U5, K2st_U6 K2st_K1, K2st_K2, K2st_K4
40.	Assembly language in malware analysis.	K2st_U1, K2st_U3, K2st_U5, K2st_U6 K2st_K1, K2st_K2, K2st_K4
41.	Static analysis as a method of identifying a malware target platform.	K2st_U1, K2st_U3, K2st_U5, K2st_U6 K2st_K1, K2st_K2, K2st_K4
42.	The role of Same Origin Policy in prevention of Web-related threats.	K2st_W1, K2st_W3, K2st_W4, K2st_W5, K2st_W6 K2st_U1, K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U15 K2st_K1, K2st_K2
43.	Protection of HTTP cookies.	K2st_W1, K2st_W3, K2st_W4, K2st_W5, K2st_W6 K2st_U1, K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U15 K2st_K1, K2st_K2
44.	Use of TLS for communication protection. Authentication. Known problems and weak spots.	K2st_W1, K2st_W3, K2st_W4, K2st_W5, K2st_W6 K2st_U1, K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U15 K2st_K1, K2st_K2
45.	Man-in-the-Browser attacks.	K2st_W1, K2st_W3, K2st_W4, K2st_W5, K2st_W6 K2st_U1, K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U15 K2st_K1, K2st_K2
46.	Cross-Site Request Forgery attacks and prevention against them.	K2st_W1, K2st_W3, K2st_W4, K2st_W5, K2st_W6 K2st_U1, K2st_U4, K2st_U5, K2st_U6, K2st_U8, K2st_U9, K2st_U10, K2st_U15 K2st_K1, K2st_K2