

IV. Internship				V. Research			VI. Final Certification
Internship Title	Semester	Weeks	Credits	Semester	Weeks	Credits	Master's Thesis
Research	4	8	12	4	12	18	

VIII. Competence Matrix


Competence Code	Competence	Module Code, Discipline Code
UC-1	Use the scientific cognition techniques in research activities, to generate and to realize innovative ideas	1.1, 1.2, 1.3, 2.3.1, 2.4, 2.6.1
UC-2	Solve research and innovative problems using advanced information technologies	1.1, 1.2, 1.3, 2.4, 2.6.2
UC-3	Ensure communication, demonstrate leadership skills, be capable of team building and developing strategic goals and objectives	1.1, 1.2, 1.3, 2.3.1, 2.3.2
UC-4	Improve innovation receptivity and innovation skills	1.1, 1.2, 1.3, 2.3.3, 2.3.4
UC-5	Predict the conditions of professional activity and solve professional problems in conditions of uncertainty	1.1, 1.2, 1.3, 2.3.3, 2.3.4
UC-6	Communicate in a foreign language in an academic, scientific, and professional environment for research and innovation activities	2.5.1, 2.6.3
UC-7	Apply psychological and pedagogical methods and information and communication technologies in education and management	2.3.1, 2.3.2
DPC-1	Design and implement information security systems and enterprise information security management systems based on international standards	1.1.1, 2.2.1
DPC-2	Identify factors affecting the current state of the information system, analyze their impact, and develop and apply mathematical models for making optimal decisions	1.1.2
DPC-3	Evaluate information systems security in order to identify potential vulnerabilities, assess risks, apply expert, active audit and information security audit methodologies	1.1.3
DPC-4	Develop and apply methods and tools to secure information and communication infrastructures, including computer networks, operating systems, virtual environments, and cloud technologies	1.2, 2.1
DPC-5	Develop and apply methods and tools to ensure the security of cyber-physical systems, industrial networks, Internet of things systems	1.2, 2.1
DPC-6	Use knowledge of current cybercrime trends and methods used by criminals to design organizational, legal, physical, and technical measures to ensure the cybersecurity of protected objects	1.3.2
DPC-7	Apply organizational and legal measures to ensure information security, based on the current regulatory framework and international standards	1.3.1
DPC-8	Mastering the design methods of information security systems and methods for assessing the sensitivity of information transmission, storage and processing systems, be able to assess the effectiveness of information security	1.3.3
SC-1	Design and analyze telecommunication networks and systems	2.1.1
SC-2	Explore methods of people processes, data, and things intelligent connection	2.1.2
SC-3	Analyze functional and system database architecture, design and implement secure client-server databases	2.1.3
SC-4	Design networks connecting various sensors, actuators, and industrial controllers	2.1.5
SC-5	Design and deploy wireless networks and services, analyze their performance	2.1.5
SC-6	Design automatic process control systems	2.1.6
SC-7	Apply methods for assessing and predicting the reliability of complex systems	2.1.6
SC-8	Use the principles and basic technologies to provide functional safety of cyber-physical systems	2.2.1
SC-9	Analyze and eliminate software vulnerabilities in information systems, apply software protection tools against malware	2.2.2
SC-10	Determine the element base, use digital and analog microelectronic components when designing information security tools	2.2.3
SC-11	Use scaling, load distribution and information flow techniques, deployment strategies and dynamic expansion to design high-load information systems	2.2.3
SC-13	Develop and apply technical tools and systems to protect information and ensure the electromagnetic compatibility of radio electronic systems	2.2.4
SC-14	Determine the appropriate model of artificial intelligence for intelligence information security systems design	2.2.4

Developed on the basis of the Model Curriculum for the specialty 7-65-0533-08 Cybersecurity, approved on 6 March 2023, registration No 7-06-05-020/mp.

¹ – Depending on the level of Russian language proficiency of foreign citizens, the volume of classroom hours may change (increase/decrease (but not less than 140 classroom hours)/exemption from studying the discipline).

² – General educational disciplines «Philosophy and Methodology of Science», «Foreign Language», «Information Technologies: Basics» are studied at the choice of a master's student. The study of general education disciplines «Philosophy and Methodology of Science», «Foreign Language» ends by the passing of the candidate exam, the general education discipline «Information Technologies: Basics» – the candidate end-of-term test.

Vice-Rector
for Academic Affairs and Educational Innovations


Alesia G. Prakharenka
29.03.2024

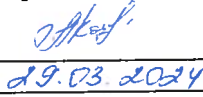
Academic Affairs Department
Head


Olga P. Rynda
29.03.2024


Dean of the Faculty of Radiophysics and Computer Technologies


Dmitrii V. Ushakov
29.03.2024

Expert norm controller


Anzhelika V. Kostenevich
29.03.2024

Department of Telecommunications and Information Technology (IT)


Yury I. Vorotnitsky
29.03.2024

Recommended for approval by the
Scientific and Methodological Board of
Belarusian State University
Record dated 29 February 2024 No. 6