

Форма обучения: очная (дневная)

Регистрационный №



II. График образовательного процесса

II. Сводные данные по бюджету времени (в неделях)

[illegible]

Обозначения: ☐ — теоретическое обучение ☒ — производственная практика ☐ // — итоговая аттестация
☐ : — экзаменационная сессия ☐ / — магистерская диссертация ☐ = — каникулы

III. План образовательного процесса

№ п/п	Название модуля, учебной дисциплины, курсового проекта (курсовой работы)	Экзамены	Зачеты	Количество академических часов						Распределение по курсам и семестрам												Всего зачетных единиц	Код компетенции	
				Всего	Аудиторных	Из них				I курс						II курс								
						Лекции	Лабораторные	Практические	Семинарские	1 семестр, 18 недель			2 семестр, 17 недель			3 семестр, 18 недель			4 семестр					
										Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов	Зач. единиц			
1.	Государственный компонент			954	396	188	120		88	414	176	12	540	220	15							27		
1.1	Модуль «Управление информационной безопасностью»																						УК-1-5	
1.1.1	Менеджмент информационной безопасности	1		90	40	24			16	90	40	3										3	УПК-1	
1.1.2	Ситуационный анализ и модели принятия решений	2		108	44	20	24						108	44	3							3	УПК-2	
1.1.3	Анализ защищенности информационных систем и аудит информационной безопасности		2	108	44	20	24						108	44	3							3	УПК-3	
1.2	Модуль «Безопасность информационно-коммуникационных технологий и систем»																						УК-1-5, УПК-4,5	
1.2.1	Киберфизические системы и их безопасность	1		108	48	24	24			108	48	3										3		
1.2.2	Безопасность компьютерных сетей и телекоммуникаций	1		108	44	20	24			108	44	3										3		
1.2.3	Безопасность операционных систем		2	108	44	20	24						108	44	3							3		
1.3	Модуль «Организационно-правовое обеспечение кибербезопасности»																						УК-1-5	
1.3.1	Организационно-правовые меры обеспечения информационной безопасности	1		108	44	20			24	108	44	3										3	УПК-7	
1.3.2	Киберпреступность и социальная инженерия	2		108	44	20			24				108	44	3							3	УПК-6	
1.3.3	Правовое регулирование и организация защиты критически важных объектов информатизации		2	108	44	20			24				108	44	3							3	УПК-8	
2.	Компонент учреждения образования			2070	694	286	264		144	594	224	18	504	132	15	990	338	30				63		
2.1	Модуль «Современные инфокоммуникационные технологии»																						УПК-4,5	
2.1.1	Системы телекоммуникаций		1	108	52	24	28			108	52	3										3	СК-1	
2.1.2	Интернет всего		1	108	48	20	20		8	108	48	3										3	СК-2	
2.1.3	Безопасность баз данных		1	90	40	20	20			90	40	3										3	СК-3	
2.1.4	Безопасность виртуальных сред и облачных технологий		2	108	44	20	24						108	44	3							3		
2.1.5	Промышленные сети / Беспроводные сети	2		108	44	16	28						108	44	3							3	СК-4 / СК-5	
2.1.6	Системы автоматического управления / Надежность сложных систем		3	90	40	20	20									90	40	3				3	СК-6 / СК-7	
2.2	Модуль «Методы и средства обеспечения кибербезопасности»																							
2.2.1	Функциональная безопасность и методы обеспечения безопасности критически важных объектов информатизации	3		90	40	16	24									90	40	3				3	УПК-1, СК-8	
2.2.2	Технологии защиты от вредоносного программного обеспечения	3		108	44	16	28									108	44	3				3	СК-9	
2.2.3	Схемотехника средств защиты информации		3	108	52	20	32									108	52	3				3	СК-10	
2.2.4	Радиофизические методы защиты информации и электромагнитная совместимость / Интеллектуальные системы защиты информации	3		198	66	26	40									198	66	6				6	СК-13 / СК-14	
2.3	Модуль «Надпрофессиональные навыки»																							
2.3.1	Методология и технологии научно-исследовательской деятельности		1	108	24	12			12	108	24	3										3	УК-1	
	Командообразование и лидерские навыки	24			12		12	24																
2.3.2	Документоведение		2	108	20	4			16				108	20	3								3	УК-3
	Деловые коммуникации	24			12		12																	
2.3.3	Экономика и управление предприятием		3	108	48	24			24							108	48	3				3	УК-4,5	
2.3.4	Риск менеджмент и обеспечение непрерывности бизнеса		3	108	48	24			24							108	48	3				3	УК-4,5	
2.4	Модуль «Научно-исследовательская работа»																						УК-1,2	
2.4.1	Исследование по направлению магистерской диссертации		1,2,3	450						90		3	180		6	180		6				15		
2.4.2	Научный семинар «Актуальные вопросы обеспечения кибербезопасности»		1	90	36				36	90	36	3										3		

№ п/п	Название модуля, учебной дисциплины, курсового проекта (курсовой работы)	Экзамены	Зачеты	Количество академических часов					Распределение по курсам и семестрам												Всего зачетных единиц	Код компетенции	
				Всего	Аудиторных	Из них				I курс						II курс							
						Лекции	Лабораторные	Практические	Семинарские	1 семестр, 18 недель			2 семестр, 17 недель			3 семестр, 18 недель			4 семестр				
										Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов			Зач. единиц
2.5	Факультативные дисциплины			/432	/280			/280		/108	/70	/3	/108	/70	/3	/108	/70	/3	/108	/70	/3	/12	
2.5.1	Русский язык как иностранный*	/4	/1,2,3	/432	/280			/280		/108	/70	/3	/108	/70	/3	/108	/70	/3	/108	/70	/3	/12	УК-6
2.6	Дополнительные виды обучения			/338	/218	/66	/24	/96	/32	/206	/138	/2	/132	/80	/7							/9	
2.6.1	Философия и методология науки	/2		/124	/72	/40			/32	/62	/40		/62	/32	/3							/3	УК-1
2.6.2	Основы информационных технологий		/1 ^а	/72	/50	/26	/24			/72	/50	/2										/2	УК-2
2.6.3	Иностранный язык	/2		/142	/96			/96		/72	/48		/70	/48	/4							/4	УК-6
Количество часов учебных занятий				3042	1090	474	384		232	1008	400	30	1044	352	30	990	338	30				90	
Количество учебных часов занятий в неделю										22			21			19							
Количество экзаменов				10						4			3			3							
Количество зачетов				17						6			6			5							

IV. Производственные практики				V. Магистерская диссертация			VI. Итоговая аттестация	
Название практики	Семестр	Неделя	Зачетных единиц	Семестр	Неделя	Зачетных единиц	Защита магистерской диссертации	
Научно-исследовательская	4	8	12	4	12	18		

VIII. Матрица компетенций

Код компетенции	Наименование компетенции	Код модуля учебной дисциплины
УК-1	Применять методы научного познания в исследовательской деятельности, генерировать и реализовывать инновационные идеи	1.1, 1.2, 1.3, 2.3.1, 2.4, 2.6.1
УК-2	Решать научно-исследовательские и инновационные задачи на основе применения информационно-коммуникационных технологий	1.1, 1.2, 1.3, 2.4, 2.6.2
УК-3	Обеспечивать коммуникации, проявлять лидерские навыки, быть способным к командообразованию и разработке стратегических целей и задач	1.1, 1.2, 1.3, 2.3.1, 2.3.2
УК-4	Развивать инновационную восприимчивость и способность к инновационной деятельности	1.1, 1.2, 1.3, 2.3.3, 2.3.4
УК-5	Быть способным к прогнозированию условий реализации профессиональной деятельности и решению профессиональных задач в условиях неопределенности	1.1, 1.2, 1.3, 2.3.3, 2.3.4
УК-6	Осуществлять коммуникации на иностранном языке в академической, научной и профессиональной среде для реализации научно-исследовательской и инновационной деятельности	2.5.1, 2.6.3
УК-7	Применять психолого-педагогические методы и информационно-коммуникационные технологии в образовании и управлении	2.3.1, 2.3.2
УПК-1	Осуществлять проектирование и внедрение систем защиты информации и систем управления информационной безопасностью предприятия на основе актов законодательства Республики Беларусь, а также международных стандартов	1.1.1, 2.2.1
УПК-2	Выявлять факторы, влияющие на текущее состояние объекта оценки, анализировать их влияние, составлять и применять математические модели принятия оптимальных решений	1.1.2
УПК-3	Осуществлять анализ защищенности информационных систем, направленный на выявление потенциальных уязвимостей, исследование и анализ рисков, связанных с возможностью осуществления угроз безопасности, применять на практике методологии экспертного, активного аудита, аудита на соответствие стандартам информационной безопасности	1.1.3
УПК-4	Разрабатывать и применять на практике методы и средства обеспечения безопасности информационно-коммуникационных инфраструктур, включая компьютерные сети, операционные системы, виртуальные среды и облачные технологии.	1.2, 2.1
УПК-5	Разрабатывать и применять на практике методы и средства обеспечения безопасности киберфизических систем, промышленных сетей, систем интернета вещей	1.2, 2.1
УПК-6	Использовать знания современных трендов киберпреступности и применяемых преступниками методов для проектирования организационно-правовых, физических и технических мер обеспечения кибербезопасности защищаемых объектов	1.3.2
УПК-7	Применять организационно-правовые меры обеспечения информационной безопасности, основываясь на нормативной правовой базе, национальных и международных стандартах	1.3.1
УПК-8	Проектировать и внедрять системы защиты информации и системы информационной безопасности критически важных объектов информатизации	1.3.3
СК-1	Проектировать сети и системы телекоммуникаций, анализировать их работу	2.1.1
СК-2	Исследовать методы интеллектуального информационно-коммуникационного соединения людей процессов, данных и вещей	2.1.2
СК-3	Анализировать функциональную и системную архитектуру баз данных в контексте обеспечения информационной безопасности, проектировать и программно реализовывать защищенные клиент-серверные базы данных	2.1.3
СК-4	Проектировать сети передачи данных, связывающие различные датчики, исполнительные механизмы и промышленные контроллеры	2.1.5
СК-5	Проектировать и разворачивать беспроводные сети и сервисы, анализировать их работу	2.1.5
СК-6	Проектировать системы автоматического управления технологическими процессами	2.1.6
СК-7	Применять методы оценки и прогнозирования надежности сложных систем	2.1.6
СК-8	Использовать принципы и базовые технологии функциональной безопасности киберфизических систем, методы управления информационной безопасностью для защиты критически важных объектов информатизации	2.2.1
СК-9	Анализировать и устранять уязвимости программного обеспечения информационных систем, применять программные средства защиты от вредоносного программного обеспечения	2.2.2
СК-10	Определять элементную базу, использовать цифровые и аналоговые микроэлектронные структуры при проектировании средств защиты информации	2.2.3
СК-13	Разрабатывать и применять технические средства и системы для защиты информации и обеспечения электромагнитной совместимости радиоэлектронных систем	2.2.4
СК-14	Определять подходящую модель организации искусственного интеллекта при проектировании систем защиты информации	2.2.4

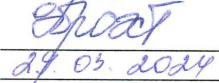
Разработан на основе Примерного учебного плана по специальности 7-06-0533-08 «Кибербезопасность», утвержденного 06.03.2023 (регистрационный № 7-06-05-020/пр.).

^а – Дифференцированный зачет.

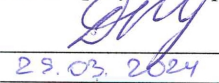
* – В зависимости от уровня владения иностранными гражданами русским языком объем аудиторных часов может изменяться (увеличение / уменьшение (но не менее 140 ауд. часов) / освобождение от изучения дисциплины).

СОГЛАСОВАНО

Проректор по учебной работе и образовательным инновациям

 О.Г.Прохоренко

Декан факультета радиофизики и компьютерных технологий

 Д.В.Ушаков

Заведующий кафедрой телекоммуникаций и информационных технологий

 Ю.И.Воротницкий

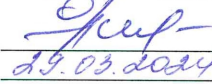
Заведующий кафедрой интеллектуальных систем

 Е.И.Козлова

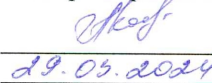
Рекомендован к утверждению научно-методическим советом
Белорусского государственного университета
протокол от 29.02.2024 № 6

СОГЛАСОВАНО

Начальник Главного управления образовательной деятельности

 О.П.Рында

Эксперт-нормоконтролер

 А.В.Костеневич