



№ 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			
Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов	Зач. единиц	Всего часов	Ауд. часов	Зач. единиц					
2.6	Дополнительные виды обучения																		
2.6.1	Философия и методология науки <sup>1</sup>	/2		/124	/72	/40			/32	/62	/40		/62	/32	/3			/3	УК-1
2.6.2	Основы информационных технологий <sup>1</sup>		/1 <sup>А</sup>	/72	/50	/26	/24			/72	/50	/2						/2	УК-2
2.6.3	Иностранный язык <sup>1</sup>	/2		/142	/96		/96			/72	/48		/70	/48	/4			/4	УК-3
<b>Количество часов учебных занятий</b>				<b>3190</b>	<b>1134</b>	<b>490</b>	<b>416</b>		<b>192</b>	<b>1026</b>	<b>408</b>	<b>30</b>	<b>1044</b>	<b>398</b>	<b>30</b>	<b>1048</b>	<b>328</b>	<b>30</b>	<b>90</b>
Количество учебных часов занятий в неделю										<b>23</b>			<b>23</b>			<b>18</b>			
Количество экзаменов					11					4			4			3			
Количество зачетов					17					6			6			5			

IV. Производственная практика				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, 2.5, 2.6.1
УК-2	Решать научно-исследовательские и инновационные задачи на основе применения информационно-коммуникационных технологий	1.1, 1.2, 1.3, 2.5, 2.6.2
УК-3	Осуществлять коммуникации на иностранном языке в академической, научной и профессиональной среде для реализации научно-исследовательской и инновационной деятельности	2.6.3
УК-4	Обеспечивать коммуникации, проявлять лидерские навыки, быть способным к командообразованию и разработке стратегических целей и задач	1.1, 1.2, 1.3, 2.3.2, 2.3.3, 2.3.4
УК-5	Развивать инновационную восприимчивость и способность к инновационной деятельности	1.1, 1.2, 1.3, 2.3.5, 2.3.6
УК-6	Быть способным к прогнозированию условий реализации профессиональной деятельности и решению профессиональных задач в условиях неопределенности	1.1, 1.2, 1.3, 2.3.5, 2.3.6
УК-7	Применять психолого-педагогические методы и информационно-коммуникационные технологии в образовании и управлении	2.3.2, 2.3.4, 2.5.1
УПК-1	Осуществлять проектирование и внедрение систем защиты информации и систем управления информационной безопасностью предприятия на основе международных стандартов и национальных нормативных правовых актов	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	1.3.1
УПК-7	Применять организационно-правовые меры обеспечения информационной безопасности, основываясь на действующей нормативной правовой базе, национальных и международных стандартах	1.3.2
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 КВОИ	2.2.1
СК-9	Анализировать и устранять уязвимости программного обеспечения информационных систем, применять программные средства защиты от вредоносного ПО	2.2.2
СК-10	Определять элементную базу, использовать цифровые и аналоговые микроэлектронные структуры при проектировании средств защиты информации	2.2.3
СК-11	Использовать приемы масштабирования, распределения нагрузки и информационных потоков, стратегии развертывания и динамического расширения для проектирования высоконагруженных информационных систем	2.2.3
СК-12	Применять методы безопасного использования открытого программного обеспечения для проектирования и разработки информационных систем	2.2.4
СК-13	Разрабатывать и применять технические средства и системы для защиты информации и обеспечения электромагнитной совместимости радиоэлектронных систем	2.2.5
СК-14	Определять подходящую модель организации искусственного интеллекта при проектировании систем защиты информации	2.2.5

Разработан в качестве примера реализации образовательного стандарта по специальности 7-06-0533-08 «Кибербезопасность».

<sup>1</sup> – Изучение общеобразовательных дисциплин «Философия и методология науки», «Иностранный язык», «Основы информационных технологий» является обязательным для магистрантов – граждан Республики Беларусь.

<sup>А</sup> – Дифференцированный зачет.

**СОГЛАСОВАНО**

Председатель УМО по естественнонаучному образованию

« 23 » 2023 г. Д.М. Курлович

Председатель УМО по компьютерной безопасности

« 23 » 2023 г. А.Н. Курбацкий

Рекомендован к утверждению Президиумом Совета УМО по естественнонаучному образованию  
Протокол № 2 от 20.02.2023 г.

**СОГЛАСОВАНО**

Начальник Главного управления профессионального образования  
Министерства образования Республики Беларусь

« 23 » 2023 г. С.Н. Пищов

« 23 » 2023 г. Экспертно-методической работе Государственного учреждения «Республиканский институт высшей школы»

« 23 » 2023 г. И.В. Титович

Эксперт-информоконтролер

« 06 » 2023 г. Д.В. Сеген

Информация об изменениях размещается на сайте:  
<http://www.edustandard.by>  
<http://www.nihe.bsu.by>