МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УТВЕРЖДАЮ
Первый заместитель
Министра образования
Республики Беларусь
_____ А.Г. Баханович
06.03.2023
Регистрационный № 7-06-05-020 /пр.

ПРИМЕРНЫЙ УЧЕБНЫЙ ПЛАН

Специальность 7-06-0533-08 Кибербезопасность

Степень: Магистр

Профилизация: Технологии и аппаратно-программные средства кибербезопасности

Срок обучения: 2 года

I. График образовательного процесса

II. Сводные данные по бюджету времени (в неделях)

КУРСЫ	сентябрь					октябрь				ноябрь				декабрь				январь				февраль				март				апрель				май				июнь				июль				август				Теоретическое обучение	Экзаменационные сессии	Производственные практики	Магистерская диссертация	Итоговая аттестация	Каникулы	Всего
	1	8	15	22	29/09	6	13	20	27/10	3	10	17	24	1	8	15	22	29/12	5	12	19	26/01	2	9	16	23/02	2	9	16	23	30/03	6	13	20	27/04	4	11	18	25	1	8	15	22	29/06	6	13	20	27/07	3	10	17	24							
	7	14	21	28	05/10	12	19	26	02/11	9	16	23	30	7	14	21	28	04/01	11	18	25	01/02	8	15	22	01/03	8	15	22	29	05/04	12	19	26	03/05	10	17	24	31	7	14	21	28	05/07	12	19	26	02/08	9	16	23	31							
I										18								:	:	:	=	=									17								:	:	:	:	=	=	=	=	=	=	=	=	35	7				10	52
II										18								:	:	=	=	X	X	X	X	X	X	X	X	/	/	/	/	/	/	/	/	/	/	/	/	//												18	2	8	12	1	2	43
																																																			53	9	8	12	1	12	95

Обозначения: [ ] — теоретическое обучение; [X] — 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: Всего	Аудиторных	Из них: Лекции	Лабораторные	Практические	Семинарские	Распределение по курсам и семестрам: I курс, 1 семестр, 18 недель: Всего часов	Ауд. часов	Зач. единиц	I курс, 2 семестр, 17 недель: Всего часов	Ауд. часов	Зач. единиц	II курс, 3 семестр, 18 недель: Всего часов	Ауд. часов	Зач. единиц	Всего зачетных единиц	Код компетенции
1.	**Государственный компонент**			**1026**	**396**	**188**	**120**		**88**	**414**	**176**	**12**	**540**	**220**	**15**				**27**	
1.1	**Модуль «Управление информационной безопасностью»**																			**УК-1,2,4-6**
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-1,2,4-6, 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-1,2,4-6**
1.3.1	Киберпреступность и социальная инженерия	1		108	44	20			24	108	44	3							3	УПК-6
1.3.2	Организационно-правовые меры обеспечения информационной безопасности	2		108	44	20			24				108	44	3				3	УПК-7
1.3.3	Правовое регулирование и организация защиты КВОИ		2	108	44	20			24				108	44	3				3	УПК-8
2.	**Компонент учреждения образования**			**2164**	**738**	**302**	**296**		**104**	**612**	**232**	**18**	**504**	**178**	**15**	**1048**	**328**	**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	52	20	24		8	108	52	3							3	СК-2
2.1.3	Безопасность баз данных		1	108	44	20	24			108	44	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	50	18	32						108	50	3				3	СК-4 / СК-5
2.1.6	Системы автоматического управления / Надежность сложных систем		2	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 КВОИ	3		90	40	16	24									90	40	3	3	УПК-1, СК-8
2.2.2	Технологии защиты от вредоносного ПО	3		108	44	16	28									108	44	3	3	СК-9
2.2.3	Схемотехника средств защиты информации / Проектирование высоконагруженных информационных систем		3	108	52	20	32									108	52	3	3	СК-10 / СК-11
2.2.4	Применение и безопасность открытого программного обеспечения		3	108	44	16	28									108	44	3	3	СК-12
2.2.5	Радиофизические методы защиты информации и электромагнитная совместимость / Интеллектуальные системы защиты информации	3		108	52	20	32									108	52	3	3	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
2.3.2	Командообразование и лидерские навыки				24	12			12		24									УК-4,7
2.3.3	Документоведение		2	108	20	8			12				108	20	3				3	УК-4
2.3.4	Деловые коммуникации				24	12			12					24						УК-4,7
2.3.5	Экономика и управление предприятием		3	108	48	24			24							108	48	3	3	УК-5,6
2.3.6	Риск менеджмент и обеспечение непрерывности бизнеса		3	108	48	24			24							108	48	3	3	УК-5,6
2.4	**Модуль «Научно-исследовательская работа»**																			**УК-1,2**
2.4.1	Исследование по направлению магистерской диссертации		1-3	490						90		3	90		3	310		9	15	
2.4.2	Научный семинар «Актуальные вопросы обеспечения кибербезопасности»		1	90	36					90	36	3							3	
2.5	**Факультативные дисциплины**																			
2.5.1	Технологии креативного образования в высшей школе / Педагогика и психология высшего образования		/1	/90	/34	/20		/14		/90	/34	/3								УК-7

№ 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
						Из них				I курс						II курс				
										1 семестр, 18 недель			2 семестр, 17 недель			3 семестр, 18 недель				
				Всего	Аудиторных	Лекции	Лабораторные	Практические	Семинарские	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[1]	/2		/124	/72	/40			/32	/62	/40		/62	/32	/3				/3	УК-1
2.6.2	Основы информационных технологий[1]		/1д	/72	/50	/26	/24			/72	/50	/2							/2	УК-2
2.6.3	Иностранный язык[1]	/2		/142	/96			/96		/72	/48		/70	/48	/4				/4	УК-3
Количество часов учебных занятий				**3190**	**1134**	**490**	**416**		**192**	**1026**	**408**	**30**	**1044**	**398**	**30**	**1048**	**328**	**30**	**90**	
Количество учебных часов занятий в неделю										**23**			**23**			**18**				
Количество экзаменов				11						4			4			3				
Количество зачетов				17						6			6			5				

IV. Производственная практика

Название практики	Семестр	Недель	Зачетных единиц
Научно-исследовательская	4	8	12

V. Магистерская диссертация

Семестр	Недель	Зачетных единиц
4	12	18

VI. Итоговая аттестация

Защита магистерской диссертации

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».

[1] – Изучение общеобразовательных дисциплин «Философия и методология науки», «Иностранный язык», «Основы информационных технологий» является обязательным для магистрантов – граждан Республики Беларусь.
д – Дифференцированный зачет.

СОГЛАСОВАНО

Председатель УМО по естественнонаучному образованию

_____ Д.М. Курлович
«__» _____ 2023 г.

Председатель НМС по компьютерной безопасности

_____ А.Н. Курбацкий
«03» 03 2023 г.

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

_____ С.Н. Пищов
«__» _____ 2023 г.

Проректор по научно-методической работе Государственного учреждения образования «Республиканский институт высшей школы»

_____ И.В. Титович
«__» _____ 2023 г.

Эксперт-нормоконтролер

_____ Д.В. Сеген
«06» 03 2023 г.

Информация об изменениях размещается на сайтах:
http://www.edustandart.by
http://www.nihe.bsu.by