МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Утверждено решением Ученого совета
Тульского государственного университета
от «31» января 2023 г., протокол № 7

Ректор _____ О.А. Кравченко

М.П.

ОБЩАЯ ХАРАКТЕРИСТИКА
основной профессиональной образовательной программы высшего образования – программы магистратуры

по направлению подготовки

10.04.01 Информационная безопасность

с направленностью (профилем)

Информационная безопасность

Идентификационный номер образовательной программы: 100401-01-23

Тула 2023 год

1 Общие сведения об образовательной программе

1.1 Реализуемая в федеральном государственном бюджетном образовательном учреждении высшего образования «Тульский государственный университет» (далее – университет) основная профессиональная образовательная программа высшего образования – программа магистратуры (далее – ОПОП ВО) по направлению подготовки 10.04.01 Информационная безопасность с направленностью (профилем) «Информационная безопасность» включает в себя общую характеристику ОПОП ВО, учебный план и календарный учебный график, рабочие программы дисциплин (модулей), практик, итоговой (государственной итоговой) аттестации, оценочные и методические материалы, а также иные компоненты, предусмотренные законодательством в сфере образования.

1.2 ОПОП ВО разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратуры (далее – ФГОС ВО) по направлению подготовки 10.04.01 «Информационная безопасность», утвержденным приказом Минобрнауки России от 26 ноября 2020 г. №1455.

1.3 Обучение по ОПОП ВО осуществляется в очной, очно-заочной формах.

1.4 Срок получения образования устанавливается учебным планом (индивидуальным учебным планом).

1.5 Объем ОПОП ВО составляет 120 зачетных единиц.

1.6 Выпускнику, освоившему ОПОП ВО, присваивается квалификация «Магистр».

1.7 Образовательная деятельность по ОПОП ВО осуществляется на государственном языке Российской Федерации.

2 Цель и задачи ОПОП ВО

2.1 Целью ОПОП ВО является обеспечение комплексной, всесторонней и качественной подготовки квалифицированных, конкурентоспособных специалистов в области информационной безопасности на основе формирования у обучающихся компетенций, определяющих уровень развития личностных качеств, а также компетенций, характеризующих способность и готовность обучающегося выполнять профессиональные функции, в соответствии с требованиями ФГОС ВО по данному направлению подготовки.

2.2 Задачами ОПОП ВО являются:

- владеющих навыками системного анализа прикладной области, выявления угроз и оценки уязвимости информационных систем, разработки требований и критериев оценки информационной безопасности;

- готовых к разработке систем, комплексов, средств и технологий обеспечения информационной безопасности;

- способны владеть методами организации и управления службами

защиты информации.

- готовых работать в конкурентоспособной среде на рынке труда в области информационной безопасности в условиях модернизации систем, средств и технологий обеспечения информационной безопасности;

- способных решать задачи в сфере профессиональной деятельности по обеспечению информационной безопасности.

3 Характеристика профессиональной деятельности выпускников, освоивших ОПОП ВО

3.1 Области профессиональной деятельности и (или) сферы профессиональной деятельности, в которых выпускники, освоившие ОПОП ВО, могут осуществлять профессиональную деятельность:

– 06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи; технической защиты информации; защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности).

Выпускники могут осуществлять профессиональную деятельность в других областях профессиональной деятельности и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

3.2 Выпускники, освоившие ОПОП ВО, готовы решать задачи профессиональной деятельности следующих типов:

– проектный;

– научно-исследовательский;

– организационно-управленческий.

3.3 Перечень основных задач и объектов (или областей знания) профессиональной деятельности выпускников, освоивших ОПОП ВО:

Область профессиональной деятельности (по Реестру Минтруда)	**Типы задач профессиональной деятельности**	**Задачи профессиональной деятельности**	**Объекты профессиональной деятельности (или области знания)**
06 Связь, информационные и коммуникационные технологии (в сферах: защиты информации в компьютерных системах и сетях, автоматизированных системах, системах и сетях электросвязи; технической защиты	Проектный	Обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных	Фундаментальные и прикладные проблемы информационной безопасности. Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и ин-

Область профессиональной деятельности (по Реестру Минтруда)	Типы задач профессиональной деятельности	Задачи профессиональной деятельности	Объекты профессиональной деятельности (или области знания)
информации; защиты значимых объектов критической информационной инфраструктуры, информационно-аналитических систем безопасности)		стандартов; Оценка уязвимости информационных систем; Разработка систем, комплексов, средств и технологий обеспечения информационной безопасности; Разработка проектов организационно-распорядительных документов, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности; Выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.	формационно-аналитические системы. Средства и технологии обеспечения информационной безопасности и защиты информации Экспертиза, сертификация и контроль защищенности информации и объектов информатизации. Методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации Организация и управление информационной безопасностью.
	Научно-исследовательский	Системный анализ фундаментальных и прикладных проблем информационной безопасности; Разработка планов и программ проведения научных исследовании и технических разработок; Выполнение научных исследований с применением соответствующих физических и математических методов;	Фундаментальные и прикладные проблемы информационной безопасности Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы. Средства и технологии обеспечения информационной безопасности и защиты информации.

Область профессиональной деятельности (по Реестру Минтруда)	Типы задач профессиональной деятельности	Задачи профессиональной деятельности	Объекты профессиональной деятельности (или области знания)
		Подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях; Разработка программ и методик испытаний средств и систем обеспечения информационной безопасности, мониторинга защищенности компьютерных систем; Выполнение исследований работоспособности и эффективности применяемых программно-аппаратных средств защиты информации.	Экспертиза, сертификация и контроль защищенности информации и объектов информатизации. Методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации. Организация и управление информационной безопасностью.
	Организационно-управленческий	Организация работ по выявлению уязвимостей; разработка требований Разработка требований и критериев оценки информационной безопасности и организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами по обеспечению за-	Фундаментальные и прикладные проблемы информационной безопасности. Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы. Средства и технологии обеспечения информационной безопасности и защиты информации; Экспертиза, сертификация и контроль защищенности информации и объектов информатизации.

Область профессиональной деятельности (по Реестру Минтруда)	Типы задач профессиональной деятельности	Задачи профессиональной деятельности	Объекты профессиональной деятельности (или области знания)
		щиты информации; Организация и выполнение аудита информационной безопасности информационных систем; Организация и выполнение работ по проведению аудита информационной безопасности и аттестации объектов информатизации по требованиям безопасности информации.	Методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации. Организация и управление информационной безопасностью.

4 Планируемые результаты освоения ОПОП ВО

4.1 Универсальные компетенции выпускника, подлежащие формированию в результате освоения ОПОП ВО, и индикаторы их достижения:

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает принципы поиска, отбора и обобщения информации.
		УК-1.2. Умеет критически анализировать проблемные ситуации и вырабатывать стратегию действий.
		УК-1.3. Владеет методами критического анализа и системного подхода для решения поставленных задач.
Разработка и реализация проектов	УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает этапы жизненного цикла проекта; виды ресурсов и ограничений для решения проектных задач; необходимые для осуществления проектной деятельности правовые нормы и принципы управления проектами.
		УК-2.2. Умеет планировать проектную деятельность, управлять проектом на всех этапах его жизненного цикла, учитывая имеющиеся ресурсы, ограничения и действующие правовые нормы.

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
		УК-2.3. Владеет методами управления проектом на всех этапах его жизненного цикла, исходя из имеющихся ресурсов и ограничений, в том числе правовых.
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Знает стадии формирования проектной команды, способы поддержания баланса интересов участников команды.
		УК-3.2. Умеет разрабатывать командную стратегию для достижения поставленной цели.
		УК-3.3. Владеет методами организации и управления коллективом.
Коммуникация	УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Знает закономерности, принципы и правила современных коммуникативных технологий для осуществления профессионального взаимодействия, в том числе на иностранном языке.
		УК-4.2. Умеет готовить материалы по результатам академической и профессиональной деятельности для представления на мероприятиях различного уровня.
		УК-4.3. Владеет навыками межличностного профессионального общения, в том числе на иностранном языке, с применением современных коммуникативных технологий
Межкультурное взаимодействие	УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Знает особенности межкультурной коммуникации в условиях современного поликультурного пространства.
		УК-5.2. Умеет осуществлять коммуникацию с представителями иных национальностей и конфессий в процессе межкультурного взаимодействия.
		УК-5.3. Владеет навыками эффективного межкультурного взаимодействия при решении профессиональных задач.
Самоорганизация и саморазвитие (в том числе здоровь-	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы	УК-6.1. Знает основные принципы саморазвития и самоорганизации; особенности профессионального и личностного развития.

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
есбережение)	ее совершенствования на основе самооценки	УК-6.2.Умеет решать задачи собственного личностного и профессионального развития; определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля.
		УК-6.3. Владеет навыками определения приоритетов личностного роста и способами совершенствования собственной деятельности.

4.2 Общепрофессиональные компетенции выпускника, подлежащие формированию в результате освоения ОПОП ВО, и индикаторы их достижения:

Наименование категории (группы) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
	ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1. Знать: требования к системе обеспечения информационной безопасности.
		ОПК-1.2. Уметь: обосновывать требования к системе обеспечения информационной безопасности.
		ОПК-1.3. Владеть: навыками разработки проектов технического задания на ее создание.
	ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1. Знать: состав, характеристики и функциональные возможности систем (подсистем) обеспечения информационной безопасности.
		ОПК-2.2. Уметь: обосновывать состав, характеристики и функциональные возможности систем (подсистем) обеспечения информационной безопасности.
		ОПК-2.3. Владеть: навыками разработки технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

Наименование категории (группы) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
	ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1. Знать: работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами.
		ОПК-3.2. Уметь: разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.
		ОПК-3.3. Владеть: навыками разработки проекты организационно-распорядительных документов по обеспечению информационной безопасности.
	ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	ОПК-4.1. Знать: фундаментальные и прикладные проблемы информационной безопасности.
		ОПК-4.2. Уметь: осуществлять сбор, обработку и анализ научно-технической информации по теме исследования.
		ОПК-4.3. Владеть: навыками разработки планов и программ проведения научных исследований и технических разработок
	ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	ОПК-5.1. Знать: физические и математические методы научных исследований для использования в профессиональной деятельности.
		ОПК-5.2. Уметь обрабатывать результаты исследований в области информационной безопасности.
		ОПК-5.3. Владеть: навыками подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях.

4.3 Профессиональные компетенции выпускника, подлежащие формированию в результате освоения ОПОП ВО, и индикаторы их достижения:

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
Профессиональные компетенции, определяемые самостоятельно разработчиками ОПОП ВО	
Тип задач профессиональной деятельности: проектный	
ПК-1. Способен разрабатывать проектные решения по защите информации в автоматизированных системах (Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (06.033), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 525н, С/02.7)	ПК-1.1. Знает руководящие, методические документы нормативные правовые акты по защите информации, национальные стандарты по лицензированию и сертификации средств защиты информации, принципы организации и структуры систем защиты информации, формирования политики информационной безопасности в автоматизированных системах, основные характеристики технических средств защиты информации от утечек по техническим каналам.
	ПК-1.2. Умеет применять действующую нормативную базу в области обеспечения защиты информации и противодействия технической разведке, определять методы управления доступом типы доступа и правила разграничения доступа к объектам, определять структуру системы защиты информации автоматизированной системы, определять виды и типы средств защиты информации, выбирать меры защиты информации.
	ПК-1.3. Владеет навыками разработки модели угроз и нарушителя безопасности в автоматизированных системах, проектов нормативных документов по защите информации, предложений по системы управления безопасностью информации в автоматизированных системах.
ПК-2. Способен разрабатывать эксплуатационную документацию на систему защиты информации автоматизированных систем (Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (06.033), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 525н, С/03.7)	ПК-2.1. Знает основные методы управления информационной безопасностью, проектами в области информационной безопасности, национальные, межгосударственные и международные стандарты, нормативные правовые акты, руководящие и методические документы в области защиты информации, основные меры по защите информации, методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системах.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
	ПК-2.2. Умеет определять меры для защиты информации, разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов, оценивать риски информационной безопасности, эффективность проектных решений по защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности автоматизированных систем.
	ПК-2.3. Владеет навыками анализа технической документации, защищенности информационной инфраструктуры автоматизированной системы, структурных и функциональных схем защищенных автоматизированных информационных систем, формирования требований по защите информации, использования программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах.
ПК-3. Способен обосновывать необходимость защиты информации в автоматизированной системе (Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (06.033), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 525н, D/01.7)	ПК-3.1. Знает основные информационные технологии, используемые в автоматизированных системах, основные угрозы безопасности информации и модели нарушителя, виды информационных воздействий и критерии оценки защищенности информации, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации, программно-аппаратные средства обеспечения защиты информации.
	ПК-3.2. Умеет выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, оценивать угрозы безопасности информации, организовывать работы по созданию, внедрению, проектированию, разработке и сопровождению защищенных автоматизированных систем.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
	ПК-3.3. Владеет навыками анализа обрабатываемой информации и определение перечня информации, подлежащей защите, планирования мероприятий по обеспечению защиты информации, определение требуемого класса (уровня) защищенности автоматизированной системы и разработки отчетных документов и разделов технических заданий.
ПК-4. Способен разрабатывать архитектуру системы защиты информации автоматизированной системы (Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (06.033), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 525н, D/03.7)	ПК-4.1. Знает основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации, программно-аппаратные средства обеспечения защиты информации, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации, организационные меры по защите информации.
	ПК-4.2. Умеет определять комплекс мер для обеспечения информационной безопасности, выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, разрабатывать предложения по совершенствованию системы управления защитой информации, проводить выбор средств обеспечения безопасности информации, разрабатывать модели угроз безопасности информации и нарушителей в автоматизированных системах.
	ПК-4.3. Владеет навыками проведения оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации, разработки технических заданий и проектной документации на создание систем защиты информации автоматизированных систем.
ПК-5. Способен проектировать объекты в защищенном исполнении (Профессиональный стандарт «Специалист по технической защите информации» (06.034), утвержденный приказом Минтруда России от 9 августа 2022 г. № 474н, H)	ПК-5.1. Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации, проектирования и сертификации средств защиты информации, аттестации объектов информатизации, порядок создания автоматизированных систем в защищенном исполнении, способы и технологии защиты технических средств обработки информации от утечки по техническим каналам, методы контроля защищенности информации от утечки по техническим каналам и несанкционированного доступа.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
	ПК-5.2. Умеет формировать требования к средствам и системам информатизации в защищенном исполнении, проводить предпроектное обследование объекта информатизации, разрабатывать аналитическое обоснование необходимости создания системы защиты информации (модель угроз безопасности информации), техническое задание, проектно-сметную, рабочую и эксплуатационную документацию, технический проект на создание средства и/или системы информатизации в защищенном исполнении, а также организационно-распорядительную документацию по защите информации.
	ПК-5.3. Владеет навыками формирования требований к средствам и системам информатизации в защищенном исполнении, разработки аналитического обоснования необходимости создания системы защиты информации (модель угроз безопасности информации), технического задания, проектно-сметной, рабочей и эксплуатационной документации, технического проекта на создание средства и/или системы информатизации в защищенном исполнении, а также организационно-распорядительной документации по защите информации.
Тип задач профессиональной деятельности: Научно-исследовательский	
ПК-6. Способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации (Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» (06.032), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 533н, С/01.7)	ПК-6.1. Знает принципы построения компьютерных систем, сетей, программно-аппаратных средств защиты информации, методы оценки эффективности политики безопасности, применяемых методов и средств защиты информации на предмет соответствия политике безопасности, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации.
	ПК-6.2. Умеет определять параметры функционирования программно-аппаратных средств защиты информации, разрабатывать и применять методики оценки защищенности программно-аппаратных средств защиты информации, оценивать эффективность защиты информации.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
	ПК-6.3. Владеет навыками оценки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.
ПК-7. Способен проводить анализ безопасности компьютерных систем (Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» (06.032), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 533н, С/03.7)	ПК-7.1. Знает принципы построения компьютерных систем, сетей, систем управления базами данных, уязвимости компьютерных систем и сетей, криптографические методы защиты информации, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации.
	ПК-7.2. Умеет анализировать компьютерную систему с целью определения уровня защищенности и доверия, проводить анализ политики безопасности на предмет адекватности, мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации, составлять и оформлять аналитический отчет по результатам проведенного анализа, формулировать предложения по устранению выявленных уязвимостей
	ПК-7.3. Владеет навыками определения уровня защищенности и доверия в компьютерных системах, оценки рисков информационной безопасности и соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, подготовки аналитического отчета по результатам проведенного оценки, формулировки предложений по устранению выявленных уязвимостей.
ПК-8. Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей (Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» (06.032), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 533н, С/05.7)	ПК-8.1. Знает принципы построения компьютерных систем и сетей, систем обнаружения компьютерных атак, формальные модели безопасности компьютерных систем и сетей, методы обработки данных мониторинга безопасности компьютерных систем и сетей, способы обнаружения и нейтрализации последствий вторжений в компьютерные системы, криптографические протоколы, применяемые в компьютерных сетях, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
	ПК-8.2. Умеет формализовать задачу управления безопасностью компьютерных систем, применять инструментальные средства проведения мониторинга защищенности компьютерных систем, методы анализа защищенности компьютерных систем и сетей, структурировать аналитическую информацию для включения в отчет.
	ПК-8.3. Владеет навыками анализа защищенности компьютерных систем с использованием сканеров безопасности, анализа защищенности сетевых сервисов с использованием средств автоматического реагирования, составления отчетов по результатам проверок.
ПК-9. Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов (Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» (06.032), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 533н, С/06.7)	ПК-9.1. Знает уязвимости компьютерных систем и сетей, технологии поиска и анализа следов компьютерных инцидентов, порядок фиксации, методы проведения расследования и документирования компьютерных инцидентов, порядок проведения экспертизы вычислительной техники и носителей компьютерной информации, порядок подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем, нормативные правовые акты, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации.
	ПК-9.2. Умеет применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа, анализировать структуру механизма возникновения и обстоятельства события, определять причину и условия изменения программного обеспечения, применять действующую законодательную базу в области обеспечения защиты информации, прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
	ПК-9.3. Владеет навыками диагностики причин, условий изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы, анализа функциональных свойств программного обеспечения, исследования алгоритма программного продукта и типов поддерживаемых аппаратных платформ, свойств исследуемой информации для определения причин, целей и условий изменений, выработки предложений по устранению выявленных уязвимостей, установления участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация, составления экспертного заключения.
ПК-10. Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации (Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (06.033), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 525н, D/04.7)	ПК-10.1. Знает методы и технологии проектирования, моделирования, исследования систем защиты информации, основные угрозы безопасности информации и модели нарушителя, меры, криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации.
	ПК-10.2. Умеет выполнять сбор, обработку, анализ и систематизацию научно-технической информации в области защиты информации, разрабатывать и исследовать математические модели конкретных явлений и процессов, применять математические модели при проектировании систем защиты информации автоматизированных систем, проектировать и реализовывать политику безопасности вычислительных сетей.
	ПК-10.3. Владеет навыками разработки, исследования аналитических и компьютерных моделей систем и подсистем безопасности автоматизированных систем, модели угроз безопасности информации и нарушителей в автоматизированных системах, исследования программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации, разработки предложений по совершенствованию системы управления информационной безопасностью.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
Тип задач профессиональной деятельности: Организационно-управленческий	
ПК-11. Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей (Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей» (06.032), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 533н, C/02.7)	ПК-11.1. Знает принципы построения компьютерных систем и сетей, средств криптографической защиты информации, модели безопасности компьютерных систем, политику безопасности компьютерных систем и сетей, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации, организационные меры по защите информации.
	ПК-11.2. Умет анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия, разрабатывать профили защиты компьютерных систем, формулировать задания по безопасности компьютерных систем, выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации и формирования политики безопасности компьютерных систем и сетей.
	ПК-11.3. Владеет навыками формирования политик безопасности компьютерных систем, разработки профилей защиты и заданий по безопасности, технических заданий на создание средств защиты информации, модели угроз безопасности информации, руководящих документов по защите информации в организации.
ПК-12. Способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой (Профессиональный стандарт «Специалист по защите информации в автоматизированных системах» (06.033), утвержденный приказом Минтруда России от 14 сентября 2022 г. № 525н, D/02.7)	ПК-12.1. Знает основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях, программно-аппаратные средства обеспечения защиты информации, основные угрозы безопасности информации и модели нарушителя, способы реализации угроз безопасности, национальные, межгосударственные и международные стандарты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области защиты информации, организационные меры по защите информации, принципы формирования и реализации политики безопасности информации.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
	ПК-12.2. Умеет производить выбор программно-аппаратных средств защиты информации, формировать перечень мероприятий по предотвращению угроз безопасности информации, систематизировать результаты проведенных исследований, анализировать выявлять уязвимости информационных систем, разрабатывать проекты нормативных документов, регламентирующих работу по защите информации.
	ПК-12.2. Владеет навыками формирования технических заданий на создание систем защиты информации, разработки систем защиты информации с учетом действующих нормативно-правовых документов, определения комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации, определения оценки возможностей внешних и внутренних нарушителей, разработки модели угроз безопасности информации, обоснование перечня сертифицированных средств защиты информации.
ПК-13. Способен проводить аттестацию объектов на соответствие требованиям по защите информации (Профессиональный стандарт «Специалист по технической защите информации» (06.034), утвержденный приказом Минтруда России от 9 августа 2022 г. № 474н, I)	ПК-13.1. Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации и аттестации объектов информатизации, технические каналы утечки информации, способы реализации несанкционированного доступа к информации, способы защиты информации от утечки по техническим каналам, методы и методики контроля защищенности информации от утечки по техническим каналам, порядок аттестации выделенных (защищаемых) помещений, отчетные документы, оформляемые по результатам аттестации объектов вычислительной техники.
	ПК-13.2. Умеет разрабатывать программы и методики аттестационных испытаний объектов вычислительной техники, выделенных защищаемых помещений, проводить аттестационные испытания объектов вычислительной техники, выделенных защищаемых помещений, оформлять материалы аттестационных испытаний, аттестат соответствия объектов вычислительной техники, выделенных защищаемых помещений требованиям по защите информации.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
	ПК-13.3. Владеет навыками разработки программы и методик аттестационных испытаний объектов вычислительной техники, выделенных (защищаемых) помещений, подготовки заключения по результатам проведения аттестационных испытаний объектов вычислительной техники, выделенных (защищаемых) помещений, подготовки заключения по результатам аттестации объектов вычислительной техники, выделенных (защищаемых) помещений на соответствие требованиям по защите информации.
ПК-14. Способен организовывать и проводить работы по защите информации в организации (Профессиональный стандарт «Специалист по технической защите информации» (06.034), утвержденный приказом Минтруда России от 9 августа 2022 г. № 474н, L)	ПРК-14.1. Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации, порядок создания автоматизированных систем в защищенном исполнении, организационно-распорядительную документацию по защите информации на объекте информатизации, технические каналы утечки информации, методы и средства защиты информации от утечки по техническим каналам, средства контроля защищенности информации от несанкционированного доступа.
	ПК-14.2. Умеет определять перечень информации (сведений) ограниченного доступа, подлежащих защите, определять условия расположения объектов информатизации относительно границ контролируемой зоны, разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации, проводить контроль (мониторинг) состояния системы защиты информации, организовывать работы по установке, настройки, техническому обслуживанию, устранению неисправностей и ремонту технических и программно-технических средств защиты информации, организовывать проведение специальных исследований и специальных проверок технических средств обработки информации ограниченного доступа.

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
	ПК-14.3. Владеет навыками определения перечня объектов информатизации и выделенных (защищаемых) помещений, проведения научных исследований по вопросам технической защиты информации, организация контроля состояния системы защиты информации, разработки предложений по совершенствованию организационных и технических мероприятий по технической защите информации и оценке их эффективности, совершенствованию системы технической защиты информации в организации, подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации по требованиям безопасности информации.

5 Карта формирования компетенций

Связи между планируемыми результатами освоения ОПОП ВО (компетенциями выпускника), формирующими их отдельными элементами ОПОП ВО (дисциплинами (модулями), практиками и т.п.) и индикаторами достижения компетенций устанавливаются нижеприведенной картой формирования компетенций.

Наименование элемента ОПОП ВО в соответствии с учебным планом	Коды компетенций, формируемых элементом ОПОП ВО	Коды индикаторов достижения компетенций, формируемых элементом ОПОП ВО
Блок 1. Дисциплины (модули)		
Обязательная часть ОПОП ВО		
Философско-методологические основания системного и критического мышления	УК-1	УК-1.1, УК-1.2, УК-1.3
Разработка, реализация и управление проектами	УК-1, УК-2, УК-3	УК-1.1, УК-1.2, УК-1.3 УК-2.1, УК-2.2, УК-2.3 УК-3.1, УК-3.2, УК-3.3
Межкультурное взаимодействие, коммуникация и саморазвитие в профессиональной деятельности	УК-4, УК-5, УК-6	УК-4.1, УК-4.2, УК-4.3, УК-5.1, УК-5.2, УК-5.3, УК-6.1, УК-6.2, УК-6.3
Иностранный язык в профессиональной деятельности	УК-4	УК-4.1, УК-4.2, УК-4.3
Технологии обеспечения информационной безопасности	ОПК-1, ОПК-4	ОПК-1.1, ОПК-1.2, ОПК-1.3 ОПК-4.1, ОПК-4.2, ОПК-4.3
Специальные разделы математики	ОПК-5, ОПК-4	ОПК-5.1, ОПК-5.2, ОПК-5.3 ОПК-4.1, ОПК-4.2, ОПК-4.3
Защищенные информационные системы	ОПК-2, ОПК-4	ОПК-2.1, ОПК-2.2, ОПК-2.3 ОПК-4.1, ОПК-4.2 ОПК-4.3
Управление информационной безо-	ОПК-3, ОПК-4	ОПК-3.1, ОПК-3.2, ОПК-3.3

Наименование элемента ОПОП ВО в соответствии с учебным планом	Коды компетенций, формируемых элементом ОПОП ВО	Коды индикаторов достижения компетенций, формируемых элементом ОПОП ВО
пасностью		ОПК-4.1, ОПК-4.2, ОПК-4.3
Часть ОПОП ВО, формируемая участниками образовательных отношений		
Защита интеллектуальной собственности	УК-4, ПК-2	УК-4.1, УК-4.2, УК-4.3 ПК-2.1, ПК-2.2, ПК-2.3
Управление интеллектуальной собственностью	УК-4, ПК-2	УК-4.1, УК-4.2, УК-4.3 ПК-2.1, ПК-2.2, ПК-2.3
Теория принятия решения	УК-3, ПК-11	УК-3.1, УК-3.2, УК-3.3 ПК-11.1, ПК-11.2, ПК-11.3
Теория игр и принятия решения	УК-3, ПК-11	УК-3.1, УК-3.2, УК-3.3 ПК-11.1, ПК-11.2, ПК-11.3
Методы искусственного интеллекта решения задач информационной безопасности	ПК-12	ПК-12.1, ПК-12.2, ПК-12.3
Представление знаний в информационных системах	ПК-12	ПК-12.1, ПК-12.2, ПК-12.3
Менеджмент инцидентов информационной безопасности	ПК-9	ПК-9.1, ПК-9.2, ПК-9.3
Защита программного обеспечения автоматизированных систем	ПК-6, ПК-10	ПК-6.1, ПК-6.2, ПК-6.3 ПК-10.1, ПК-10.2, ПК-10.3
Теория систем и системный анализ	УК-1, ПК-4	УК-1.1, УК-1.2, УК-1.3 ПК-4.1, ПК-4.2, ПК-4.3
Исследование операций	УК-1, ПК-4	УК-1.1, УК-1.2, УК-1.3 ПК-4.1, ПК-4.2, ПК-4.3
Физические основы защиты информации	ПК-13	ПК-13.1, ПК-13.2, ПК-13.3
Безопасность облачных технологий	ПК-6, ПК-10	ПК-6.1, ПК-6.2, ПК-6.3 ПК-10.1, ПК-10.2, ПК-10.3
Защищенные операционные системы	ПК-6, ПК-10	ПК-6.1, ПК-6.2, ПК-6.3 ПК-10.1, ПК-10.2, ПК-10.3
Проектирование и эксплуатация систем защиты информации	ПК-1, ПК-5	ПК-1.1, ПК-1.2, ПК-1.3 ПК-5.1, ПК-5.2, ПК-5.3
Технические методы и средства обеспечения информационной безопасности	ПК-14	ПК-14.1, ПК-14.2, ПК-14.3
Методы и средства обеспечения сетевой безопасности	ПК-3	ПК-3.1, ПК-3.2, ПК-3.3
Комплексная оценка безопасности автоматизированных систем	ПК-7, ПК-8	ПК-7.1, ПК-7.2, ПК-7.3 ПК-8.1, ПК-8.2, ПК-8.3
Основы теории информационной безопасности	ПК-3	ПК-3.1, ПК-3.2, ПК-3.3
Блок 2. Практика		
Обязательная часть ОПОП ВО		
Производственная практика (научно-исследовательская работа) (1 семестр)	УК-4, ОПК-4, ОПК-5	УК-4.1, УК-4.2, УК-4.3 ОПК-4.1, ОПК-4.2, ОПК-4.3 ОПК-5.1, ОПК-5.2, ОПК-5.3
Производственная практика (науч-	ОПК-1, ОПК-3,	ОПК-1.1, ОПК-1.2, ОПК-1.3

Наименование элемента ОПОП ВО в соответствии с учебным планом	Коды компетенций, формируемых элементом ОПОП ВО	Коды индикаторов достижения компетенций, формируемых элементом ОПОП ВО
но-исследовательская работа) (2 семестр)	ОПК-4	ОПК-3.1, ОПК-3.2, ОПК-3.3 ОПК-4.1, ОПК-4.2, ОПК-4.3
Производственная практика (проектно-технологическая практика)	УК-3, ОПК-2, ОПК-4	УК-3.1, УК-3.2, УК-3.3 ОПК-2.1, ОПК-2.2, ОПК-2.3 ОПК-4.1, ОПК-4.2, ОПК-4.3
Часть ОПОП ВО, формируемая участниками образовательных отношений		
Производственная практика (научно-исследовательская работа) (3 семестр)	ПК-2, ПК-6, ПК-10	ПК-2.1, ПК-2.2, ПК-2.3 ПК-6.1, ПК-6.2, ПК-6.3 ПК-10.1, ПК-10.2, ПК-10.3
Производственная практика (преддипломная практика)	ПК-1, ПК-5, ПК-7, ПК-8	ПК-1.1, ПК-1.2, ПК-1.3 ПК-5.1, ПК-5.2, ПК-5.3 ПК-7.1, ПК-7.2, ПК-7.3 ПК-8.1, ПК-8.2, ПК-8.3
Блок 3. Государственная итоговая аттестация		
Подготовка к процедуре защиты и защита выпускной квалификационной работы	УК-1, УК-2, УК-3, УК-4, УК-5, УК-6, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-12, ПК-13, ПК-14	УК-1.1, УК-1.2, УК-1.3, УК-2.1, УК-2.2, УК-2.3 УК-3.1, УК-3.2, УК-3.3 УК-4.1, УК-4.2, УК-4.3 УК-5.1, УК-5.2, УК-5.3 УК-6.1, УК-6.2, УК-6.3 ОПК-1.1, ОПК-1.2, ОПК-1.3 ОПК-2.1, ОПК-2.2, ОПК-2.3 ОПК-3.1, ОПК-3.2, ОПК-3.3 ОПК-4.1, ОПК-4.2, ОПК-4.3 ОПК-5.1, ОПК-5.2, ОПК-5.3 ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3 ПК-3.1, ПК-3.2, ПК-3.3 ПК-4.1, ПК-4.2, ПК-4.3 ПК-5.1, ПК-5.2, ПК-5.3 ПК-6.1, ПК-6.2, ПК-6.3 ПК-7.1, ПК-7.2, ПК-7.3 ПК-8.1, ПК-8.2, ПК-8.3 ПК-9.1, ПК-9.2, ПК-9.3 ПК-10.1, ПК-10.2, ПК-10.3 ПК-11.1, ПК-11.2, ПК-11.3 ПК-12.1, ПК-12.2, ПК-12.3 ПК-13.1, ПК-13.2, ПК-13.3 ПК-14.1, ПК-14.2, ПК-14.3
Факультативные дисциплины (модули)		
Методология научных исследований	УК-1	УК-1.1, УК-1.2, УК-1.3
Менеджмент командной работы	УК-3	УК-3.1, УК-3.2, УК-3.3

6 Сведения о кадровых условиях реализации ОПОП ВО

Кадровые условия реализации ОПОП ВО отвечают требованиям соответствующего ФГОС ВО.

7 Коллектив разработчиков ОПОП ВО

Научно-педагогические работники университета

Токарев В.Л.
проф. кафедры ИБ, д.т.н., доцент _____

Сычугов А.А.
зав. кафедрой ИБ, к.т.н., доцент _____

Борзенкова С.Ю.
доцент каф. ИБ, к.т.н _____

Представители профильных организаций (предприятий)

Куприянов А.О.
ОАО «Велес», генеральный директор _____
(подпись, печать организации)

Куликов В.В.
ЗАО «ЛИМ», генеральный директор,
к.т.н., доцент _____
(подпись, печать организации)

25

8 Лист согласования

Общая характеристика ОПОП ВО согласована с дирекцией (Института прикладной математики и компьютерных наук:

Директор ИПМКН _____ А.А. Сычугов

Общая характеристика ОПОП ВО согласована с УМУ:

Начальник УМУ _____ А.В. Моржов

И.о. начальника ОСУП УМУ _____ С.В. Моржова