Аннотация к рабочим программам модулей

Институт	ИРИТ-РТФ
Направление (код, наименование)	10.04.01 Информационная безопасность
Образовательная программа (Магистерская программа)	10.04.01/22.01 Защита информации в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры
Описание образовательной программы	Основная образовательная программа «Защита информации в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры», реализуемая ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина» по направлению подготовки 10.04.01 Информационная безопасность, разработана на основе требований Федерального государственного образовательного стандарта высшего образования (ФГОС ВО 3++), утвержденного Министерством науки и высшего образования Российской Федерации приказ от 26 ноября 2020 г. N 1455, описывает общие требования к результатам освоения программы, соответствуя характеристике будущей профессиональной деятельности выпускника, а также определяет модульную структуру и условия реализации образовательной программы. Основная образовательная программа магистратуры реализуется совместно с «Московским физико-техническим институтом (национальный исследовательский университет)» (МФТИ).

№ п/п	Наименования дисциплин (модулей)	Аннотации модулей
1.	**Модули**	
2.	**Обязательная часть**	
3.	Управление информационной безопасностью информационных систем персональных данных, государственных информационных систем и значимых объектах критической информационной инфраструктуры	Целью модуля является приобретение новых и/или совершенствование существующих компетенций учащихся в сфере управления информационной безопасностью систем. В модуле изучаются методы и средства управления информационной безопасностью в организации; современные подходы к проектной деятельности и средства разработки проектов в области ИБ; элементы разработки систем управления информационной безопасности (СУИБ) в государственных информационных системах; разработка системы защиты информации информационной системы; требования к мерам защиты информации, содержащейся в информационной системе; требования к организации защиты информации в автоматизированной системе управления; основные международные и национальные стандарты в области управления информационной безопасностью на основе информационной системы; управление информационными рисками как базовый процесс функционирования СУИБ; основные математические модели и методы управления информационными рисками; процессы и методы управления проектами; проектирование безопасного программного обеспечения. В модуль входят: - Управление информационной безопасностью ИСПДн, ГИС и значимых объектов КИИ; - Управление проектами в области информационной безопасности.

4.	Защищенные информационные системы	Целью модуля является формирование знаний и умений в области аудита информационной безопасности систем и средств организации защищенных сетевых коммуникаций, их аттестации по требованиям безопасности информации, организации их развертывания и модернизации, выбора оптимального решения при построении информационной системы (ИС) в зависимости от требований, предъявляемых к ее безопасности и функциональным возможностям. В модуле изучаются особенности организации защищенных сетевых коммуникаций в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры; защитные механизмы телекоммуникационного оборудования; средства терминального доступа; средства организации виртуальных частных сетей; средства межсетевого экранирования; основы пользовательской работы и администрирования защищенной операционной системы; мандатное управление доступом (МУД); мандатный контроль целостности, управление доступом к объектам графической подсистемы, особенности аутентификации и аудита. Студенты проектируют безопасные проводные и беспроводные телемеханические системы, и специализированные вычислительные сети. В модуль входят: - Организация защищенных сетевых коммуникаций в ИСПДн, ГИС и на объектах КИИ; - Методология проектирования защищенных информационных систем; - Защита информации в системах беспроводной связи.
5.	Математические методы информационной безопасности	Целью модуля является формирование знаний у умений в области анализа и прогнозирования различных практических процессов и явлений из области информационной безопасности. В модуле изучаются технологии управления большими данными, пакеты прикладных программ для решения типовых задач теории сигналов и систем, специальные математические методы обработки данных, их анализ и прогнозирование. Дисциплина «Безопасность автоматизированных систем» систематизирует математические методы и математические модели для применяемые в научно-исследовательской деятельности магистра. Знание и применение математических методов позволяют построить абстрактную модель и провести анализ угроз в области информационной безопасности. В модуль входят: - Математические методы теории сигналов и систем; - Специальные разделы математики; - Методы и инструменты анализа больших данных; - Безопасность автоматизированных информационно-управляющих систем.
6.	Гуманитарные аспекты информационной безопасности	Целью модуля является формирование знаний правовых аспектов информационной безопасности, формирование навыка владения иностранным языком на уровне достаточном для решения профессиональных задач. Модуль раскрывает философские и теоретико-методологические основы научного знания, методические принципы, а также инструментарий современных междисциплинарных научных исследований. В модуле изучаются методологии, стратегии и технологии научного исследования, Правовые аспекты информационной безопасности информационных систем персональных данных, государственных информационных систем и значимых объектов критической информационной инфраструктуры, изучается специальная лексика иностранного языка, культурных особенностей различных национальностей и стран применительно к научной и профессиональной коммуникации. В модуль входят: - Актуальные проблемы философии и истории науки; - Основы научного исследования;

		- Профессиональный иностранный язык; - Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых объектов КИИ.
7.	Методы и средства защиты информации в информационных системах персональных данных, государственных информационных системах и значимых объектах критической информационной инфраструктуры	Целью модуля является приобретение новых и/или совершенствование существующих компетенций учащихся в сфере информационной безопасности. Изучаются требования к мерам защиты информации от несанкционированного доступа и принцип их выбора; установка, настройка и администрирование средств защиты информации от несанкционированного доступа; оценивание и инструментальные средства анализа защищенности компьютерных систем, экспертное оценивание трудно формализуемых свойств (параметров); методы и стандарты оценки защищённости, правовые аспекты ИСПДн, ГИС и значимых объектов КИИ. В модуль входят: - Меры и средства защиты информации от несанкционированного доступа (НСД) в ИСПДн, ГИС и значимых объектах КИИ; - Методы контроля защищенности информации ИСПДн, ГИС и значимых объектов КИИ; - Стандарты и методы оценки защищенности ИСПДн, ГИС и значимых объектов КИИ.
8.	Криптографические методы защиты информации	Целью модуля является изучение принципов построения алгоритмов и протоколов, обеспечивающих безопасность информации, освоение принципов организации и обеспечения работы шифровальных средств, математические методы криптоанализа а также знание нормативно-правовой документации в области применения средств криптографической защиты информации. В модуль входят: - Криптографические алгоритмы и протоколы; - Криптографические методы и средства защиты в ИСПДн, ГИС и значимых объектах КИИ.
9.	**Формируемая участниками образовательных отношений**	
10.	Организация и функционирование центров мониторинга Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак	Целью модуля является формирование знаний и умений в областях экспертно-аналитической деятельности, ликвидации последствий компьютерных инцидентов и обеспечения функционирования технических средств в рамках функционирования центров мониторинга государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее — ГосСОПКА). В модуль входят: - Анализ событий безопасности и обеспечение функционирования технических средств сегмента ГосСОПКА; - Реагирование и ликвидация последствий компьютерных инцидентов в рамках функционирования центров мониторинга ГосСОПКА; - Экспертно-аналитическая деятельность в центрах мониторинга ГосСОПКА.
11.	Обнаружение и предупреждение компьютерных атак на объектах критической	Целью модуля является формирование знаний и умений в области противодействия компьютерной преступности, решения задач в области в области установки, настройки и эксплуатации систем обнаружения компьютерных атак на значимых объектах критической информационной инфраструктуры (далее КИИ), реагирования на компьютерные инциденты на значимых объектах КИИ, а также проектирования базы правил для обнаружения и предупреждения направленных компьютерных атак, формирование рекомендаций по принятию мер, направленных на недопущение повторений подобных инцидентов в будущем.

	информационной инфраструктуры	В модуле изучаются основные подходы к организации экспертно-аналитической деятельности в сфере обеспечения безопасности объектов КИИ; принципы аналитической работы с системами обнаружения атак (далее — СОА) при помощи систем управления базами данных (далее — СУБД); стандарты и нормативные правовые акты, описывающие порядок реагирования на компьютерные инциденты на значимых объектах КИИ; требования, предъявляемые к системам обнаружения компьютерных атак при защите значимых объектов КИИ; механизмы компьютерного следообразования; принципы функционирования и построения систем обнаружения компьютерных атак; ликвидация последствий компьютерного инцидента и совершенствование применяемых мер защиты. В модуль входят: - Эксплуатация систем обнаружения компьютерных атак на объектах КИИ; - Реагирование на компьютерные инциденты, ликвидация их последствий на объектах КИИ; - Экспертная и аналитическая деятельность в сфере обеспечения безопасности объектов КИИ.
12.	**Блок 2. Практика**	
13.	Производственная практика, научно-исследовательская работа	Научно-исследовательская работа (НИР) является базой для выполнения студентом выпускной квалификационной работы – магистерской диссертации. Рассматриваются современные методы выполнения НИР по проектированию и разработке конструкций узлов и комплексов радиоэлектронных средств, осваиваются принципы организации и проведения теоретических и экспериментальных работ, приобретаются необходимые навыки по созданию изделий новой техники, приобретается опыт управления результатами научно-исследовательской деятельности и коммерциализация прав на объекты интеллектуальной собственности.
14.	Производственная практика, технологическая практика	Технологическая практика является средством связи теоретического обучения с практической деятельностью, обеспечивающим прикладную направленность и специализацию обучения. Производственная практика проводится в лабораториях кафедры или на предприятиях, или организациях, соответствующих целевому направлению специальности. Во время производственного этапа используются виртуальные практикумы и оборудование предприятия, значительное внимание уделяется поисковым и исследовательским работам.
15.	Производственная практика, преддипломная практика	Целью практики является выполнение квалификационной научно-исследовательской работы, направленной на выполнение индивидуального задания на выпускную квалификационную работу (ВКР). ВКР может выполняться в интересах предприятия, на котором студент проходит практику.
16.	**Блок 3. Государственная итоговая аттестация**	
17.	Государственная итоговая аттестация	Целью государственной итоговой аттестации является комплексная оценка усвоения выпускниками образовательной программы в соответствие с требованиями Федерального государственного образовательного стандарта высшего образования (ФГОС ВО 3++) - магистратура по направлению подготовки 10.04.01 «Информационная безопасность». В рамках государственной итоговой аттестации проверяется уровень сформированности результатов освоения образовательной программы.
18.	**Факультативы**	
19.	Адаптационный модуль для лиц с ограниченными возможностями здоровья	Адаптационный модуль для обучающихся с ограниченными возможностями здоровья направлен на формирование практических навыков адаптации и социализации: осознанной саморегуляции, самопрезентации, стабилизации самооценки и межличностного взаимодействия Модуль включает в себя две дисциплины: Основы личностного роста и Развитие ресурсов организма. Курс «Основы личностного роста (для лиц с ОВЗ)» направлен на формирование гармоничной личности, адаптированной к социальному взаимодействию в высшем учебном заведении. Зрелость и гармоничность личности определяется адекватной реакцией на внешнее

		воздействие, а также умением эффективно взаимодействовать с окружающими. Для успешного взаимодействия с окружающими людьми, прежде всего, необходимо адекватно оценить собственные преимущества и недостатки. Принимая во внимания, что курс рассчитан на лиц с ограниченными возможностями здоровья, отдельное внимание уделяется психологическим особенностям обучающихся с различными нозологиями. Закономерно, что наличие инвалидности влияет не только на восприятие человека окружающими, но и на его отношение к себе. Курс «Развитие ресурсов организма (для лиц с ОВЗ)» направлен на приобретение навыков мобилизации и оптимизации индивидуальных возможностей обучающегося. Во время взросления человек испытывает максимальное напряжение и стресс, которые могут привести к снижению мотивации, эффективности деятельности и нервному срыву. Процесс адаптации обучающихся является серьезным испытанием для организма.