Матрица компетенций и планируемые результы обучения по программе
10.05.01 Специализация №6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" очная форма обучения 2025 г.н.

Индекс	Блок/ часть	Наименование	Формируемые компетенции
Б1		Дисциплины (модули)	УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; УК-7; УК-8; УК-9; УК-10; ОПК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ОПК-6; ОПК-7; ОПК-8; ОПК-9; ОПК-10; ОПК-11; ОПК-12; ОПК-13; ОПК-14; ОПК-15; ОПК-16; ОПК-17; ОПК-6.1; ОПК-6.2; ОПК-6.3; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Б1.О		Обязательная часть	УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; УК-7; УК-8; УК-9; УК-10; ОПК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ОПК-6; ОПК-7; ОПК-8; ОПК-9; ОПК-10; ОПК-11; ОПК-12; ОПК-13; ОПК-14; ОПК-15; ОПК-16; ОПК-17; ОПК-6.1; ОПК-6.2; ОПК-6.3; ПК-1
Б1.О.01	Б1.О	Алгебра	ОПК-3
Б1.О.02	Б1.О	Математический анализ	ОПК-3
Б1.О.03	Б1.О	Геометрия	ОПК-3
Б1.О.04	Б1.О	Теория вероятностей и математическая статистика	ОПК-3
Б1.О.05	Б1.О	Дискретная математика	ОПК-3
Б1.О.06	Б1.О	Дифференциальные уравнения	ОПК-3
Б1.О.07	Б1.О	Теория информации	ОПК-3
Б1.О.08	Б1.О	Аппаратные средства вычислительной техники	ОПК-4
Б1.О.09	Б1.О	Физика	ОПК-4
Б1.О.10	Б1.О	Сети и системы передачи информации	ОПК-4
Б1.О.11	Б1.О	Информатика	ОПК-2
Б1.О.12	Б1.О	Языки программирования	ОПК-7
Б1.О.13	Б1.О	Языки Ассемблера	ОПК-7
Б1.О.14	Б1.О	Системное программирование	ОПК-7; ОПК-13
Б1.О.15	Б1.О	Языки программирования Java	ОПК-7
Б1.О.16	Б1.О	Операционные системы	ОПК-12
Б1.О.17	Б1.О	Компьютерные сети	ОПК-15
Б1.О.18	Б1.О	Беспроводные сети	ОПК-15
Б1.О.19	Б1.О	Системы управления базами данных	ОПК-14
Б1.О.20	Б1.О	Основы информационной безопасности	ОПК-1; ОПК-5
Б1.О.21	Б1.О	Организационное и правовое обеспечение информационной безопасности	УК-10; ОПК-5; ОПК-6
Б1.О.22	Б1.О	Теория чисел	ОПК-3
Б1.О.23	Б1.О	Модели безопасности компьютерных систем	ОПК-8; ОПК-11
Б1.О.24	Б1.О	Методы и средства криптографической защиты информации	ОПК-10
Б1.О.25	Б1.О	Криптографические протоколы	ОПК-10
Б1.О.26	Б1.О	Основы построения защищенных компьютерных се	ОПК-9; ОПК-16
Б1.О.27	Б1.О	Основы построения защищенных баз данных	ОПК-9; ОПК-16
Б1.О.28	Б1.О	Защита информации от утечки по техническим каналам	ОПК-6; ОПК-9
Б1.О.29	Б1.О	Защита в операционных системах	ОПК-9; ОПК-13

Индекс	лок/ част	Наименование	Формируемые компетенции
Б1.О.30	Б1.О	Защита программ и данных	ОПК-13; ОПК-16
Б1.О.31	Б1.О	Введение в специальность	ОПК-1; ПК-1
Б1.О.32	Б1.О	Дисциплины(модули) специализации	ОПК-6.1; ОПК-6.2; ОПК-6.3
Б1.О.32.01	Б1.О	Основы компьютерной криминалистики	ОПК-6.3
Б1.О.32.02	Б1.О	Экспертиза вычислительной техники и компьютерных носителей информации	ОПК-6.2
Б1.О.32.03	Б1.О	Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов	ОПК-6.1
Б1.В		Часть, формируемая участниками образовательных отношений	УК-1; УК-2; УК-4; УК-7; УК-10; ПК-2; ПК-3; ПК-4; ПК-5
Б1.В.01	Б1.В	Тестирование компьютерных систем на проникновения	ПК-2
Б1.В.02	Б1.В	Методы и стандарты оценки защищенности компьютерных систем	ПК-3
Б1.В.03	Б1.В	Методы верификации	ПК-3
Б1.В.ДВ.01	Б1.В	Элективные дисциплины (модули) 1	ПК-2
Б1.В.ДВ.01.01	Б1.В	Защита IoT сетей	ПК-2
Б1.В.ДВ.01.02	Б1.В	Сетевые технологии	ПК-2
Б1.В.ДВ.02	Б1.В	Элективные дисциплины (модули) 2	ПК-3
Б1.В.ДВ.02.01	Б1.В	Дополнительные главы криптографии	ПК-3
Б1.В.ДВ.02.02	Б1.В	Исследование вредоносного программного обеспечения	ПК-3
К.М		Комплексные модули	УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; УК-7; УК-8; УК-9; УК-10; ОПК-3; ОПК-4; ОПК-7; ОПК-8; ОПК-10; ОПК-12; ОПК-17; ПК-3; ПК-5
К.М.01	К.М	Системное и критическое мышление и информационные технологии	УК-1; ОПК-3; ОПК-7; ОПК-8; ОПК-10; ПК-3
К.М.01.01	Б1.О	Философия	УК-1
К.М.01.02	Б1.О	Сбор данных из открытых источников (научный семинар)	УК-1; ОПК-7
К.М.01.03	Б1.О	Теоретико-числовые методы в криптографии	УК-1; ОПК-10
К.М.01.04	Б1.О	Искусственный интеллект (научный семинар)	УК-1; ОПК-7; ОПК-8
К.М.01.05	Б1.О	Нечеткие модели и их приложения	УК-1; ОПК-3
К.М.02	К.М	Управление проектами	УК-2; УК-3; УК-6; УК-9; УК-10; ОПК-7; ПК-5
К.М.02.01	Б1.В	Правоведение	УК-1; УК-10
К.М.02.02	Б1.О	Экономика	УК-9
К.М.02.03	Б1.О	Языки программирования Python	УК-2; ОПК-7
К.М.02.04	Б1.О	Параллельное программирование	УК-2; ОПК-7
К.М.02.05	Б1.О	Методы программирования	УК-2; ОПК-7
К.М.02.06	Б1.О	Web-программирование	УК-2; ОПК-7

Индекс	лок/ част	Наименование	Формируемые компетенции
К.М.02.07	Б1.О	Технологии программирования	УК-2; ОПК-7
К.М.02.08	Б1.О	Основы управленческой деятельности	УК-2; УК-3; УК-6
К.М.02.09	Б1.В	Управление IT-проектами	УК-2; ПК-5
К.М.03	К.М	Коммуникация и межкультурное взаимодействие	УК-4; УК-5; ОПК-4; ОПК-12; ОПК-17
К.М.03.01	Б1.О	История России	УК-5; ОПК-17
К.М.03.02	Б1.О	Культура речи и деловое общение	УК-4
К.М.03.03	Б1.О	Иностранный язык	УК-4
К.М.03.04	Б1.О	Электроника и схемотехника	УК-4; ОПК-4
К.М.03.05	Б1.О	Администрирование Windows	УК-4; ОПК-12
К.М.03.06	Б1.О	Администрирование Linux и защита публичных слу	УК-4; ОПК-12
К.М.03.07	Б1.В	Защита web-приложений	УК-4; ПК-4
К.М.03.08	Б1.О	Основы российской государственности	УК-5
К.М.04	К.М	Безопасность жизнедеятельности и здоровьесбережение	УК-7; УК-8
К.М.04.01	Б1.О	Физическая культура и спорт	УК-7
К.М.04.02	Б1.О	Безопасность жизнедеятельности	УК-8
К.М.04.ДВ.01	Б1.В	Элективные дисциплины (модули) по физической культуре и спорту	
К.М.04.ДВ.01.01	Б1.В	Прикладная физическая культура	УК-7
К.М.04.ДВ.01.02	Б1.В	Оздоровительная физическая культура	УК-7
Б2		Практика	ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Б2.О		Обязательная часть	ОПК-7; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Б2.О.01	Б2.О	Учебная практика	ОПК-7; ПК-3
Б2.О.01.01(У)	Б2.О	Учебная практика (учебно-лабораторный практику	ОПК-7; ПК-3
Б2.О.02	Б2.О	Производственная практика	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Б2.О.02.01(П)	Б2.О	Производственная практика (научно-исследовательская работа)	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Б2.О.02.02(П)	Б2.О	Производственная практика (технологическая практика)	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Б2.О.02.03(П)	Б2.О	Производственная практика (преддипломная практика)	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Б2.В		Часть, формируемая участниками образовательных отношений	
Б3		Государственная итоговая аттестация	УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; УК-7; УК-8; УК-9; УК-10; ОПК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ОПК-6; ОПК-7; ОПК-8; ОПК-9; ОПК-10; ОПК-11; ОПК-12; ОПК-13; ОПК-14; ОПК-15; ОПК-16; ОПК-17; ОПК-6.1; ОПК-6.2; ОПК-6.3; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
Б3.01(Г)	Б3	Подготовка к сдаче и сдача государственного экзамена	ОПК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ОПК-6; ОПК-7; ОПК-8; ОПК-9; ОПК-10; ОПК-11; ОПК-12; ОПК-13; ОПК-14; ОПК-15; ОПК-16; ОПК-17; ОПК-6.1; ОПК-6.2; ОПК-6.3; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5

Индекс	лок/ част	Наименование	Формируемые компетенции
Б3.02(Д)	Б3	Подготовка к процедуре защиты и защита выпускной квалификационной работы	УК-1; УК-2; УК-3; УК-4; УК-5; УК-6; УК-7; УК-8; УК-9; УК-10; ОПК-1; ОПК-2; ОПК-3; ОПК-4; ОПК-5; ОПК-6; ОПК-7; ОПК-8; ОПК-9; ОПК-10; ОПК-11; ОПК-12; ОПК-13; ОПК-14; ОПК-15; ОПК-16; ОПК-17; ОПК-6.1; ОПК-6.2; ОПК-6.3; ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
ФТД		Факультативные дисциплины	ОПК-3; ОПК-10; ПК-5
ФТД.01	ФТД	Технология программирования и работы на ЭВМ	ПК-5
ФТД.02	ФТД	Линейные рекуррентные последовательности	ОПК-3; ОПК-10

Планируемые результаты обучения по программе
10.05.01 Компьютерная безопасность, специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»
очная форма обучения, 2025 г. н.

Дисциплина		Код и содержание компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
Блок 1 Дисциплины (модули)				
Б1.О Обязательная часть				
Б1.О.01	Алгебра	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1 Знает основные свойства важнейших алгебраических систем: групп, колец, полей; основы линейной алгебры и важнейшие свойства векторных пространств над произвольными полями; основные свойства колец многочленов над кольцами и полями; основные свойства отображений важнейших алгебраических систем. ОПК-3.2 Умеет производить стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также оперировать с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; решать системы линейных уравнений над полями, приводить матрицы и квадратичные формы к каноническому виду; производить оценку качества полученных решений прикладных задач. ОПК-3.3 Владеет методами решения стандартных алгебраических, матричных, подстановочных уравнений в алгебраических структурах;	Знать: – основные понятия и методы алгебры. Уметь: – использовать алгебраические методы и модели для решения прикладных задач; – решать типовые задачи по алгебре, – выполнять операции с алгебраическими объектами. Владеть: – алгебраическими методами решения прикладных задач; – навыками решения типовых линейных уравнений; – навыками решения стандартных задач в векторных пространствах; – методами нахождения канонических форм линейных преобразований.

			навыками решения типовых линейных уравнений над полем и кольцом вычетов; навыками решения стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований.	
Б1.О.02	Математический анализ	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1 знает основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных; знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных; знает основные методы интегрального исчисления функций одной и нескольких действительных переменных; знает основные методы исследования числовых и функциональных рядов; знает основные задачи теории функций комплексного переменного; основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных; умеет обосновывать основные методы дифференциального исчисления функций одной и нескольких действительных переменных; умеет обосновывать основные методы интегрального исчисления функций одной и нескольких действительных переменных; умеет обосновывать основные	Знать: Для освоения ОПК-3.1: – знает основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных; – знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных; – знает основные методы интегрального исчисления функций одной и нескольких действительных переменных; – знает основные методы исследования числовых и функциональных рядов; – знает основные задачи теории функций комплексного переменного Уметь: Для освоения ОПК-3.2: – умеет обосновывать основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных; – умеет обосновывать основные методы дифференциального исчисления функций одной и нескольких действительных переменных; – умеет обосновывать основные методы интегрального исчисления функций одной и нескольких действительных переменных; – умеет обосновывать основные методы исследования числовых и функциональных рядов Владеть: Для освоения ОПК-3.3: – владеет навыками использования справочных материалов по математическому анализу.

			методы исследования числовых и функциональных рядов; ОПК-3.3 владеет навыками использования справочных материалов по математическому анализу.	
Б1.О.03	Геометрия	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1. Знает основные задачи векторной алгебры и аналитической геометрии; возможности координатного метода для исследования различных геометрических объектов; основные виды уравнений простейших геометрических объектов. ОПК-3.2.Умеет решать основные задачи линейной алгебры; решать основные задачи аналитической геометрии на плоскости и в пространстве. ОПК-3.3.1 Владеет навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике.	Знать: Для достижения ОПК-3.1: – основные задачи векторной алгебры и аналитической геометрии; возможности координатного метода для исследования различных геометрических объектов; – основные виды уравнений простейших геометрических объектов Уметь: Для достижения ОПК-3.2: – решать основные задачи аналитической геометрии на плоскости и в пространстве Владеть: Для достижения ОПК-3.3: – навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах.
Б1.О.04	Теория вероятностей и математическая статистика	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1 Знает основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства; классические предельные теоремы теории вероятностей; основные понятия теории случайных процессов; постановку задач и основные понятия математической статистики; стандартные методы получения точечных и интервальных оценок	Знать: – аппарат теории вероятностей и математической статистики; – основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства; – классические предельные теоремы теории вероятностей; – основные понятия теории случайных процессов; – постановку задач и основные понятия математической статистики; – стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений; – стандартные методы проверки статистических гипотез. Уметь: – применять аппарат теории вероятностей и математической

			параметров вероятностных распределений; стандартные методы проверки статистических гипотез. ОПК-3.2 Умеет обосновывать классические положения и стандартные методы теории вероятностей и случайных процессов; обосновывать классические положения и стандартные методы математической статистики; умеет разрабатывать и использовать вероятностные и статистические модели при решении типовых прикладных задач.	статистики; – обосновывать классические положения и стандартные методы теории вероятностей и случайных процессов; – обосновывать классические положения и стандартные методы математической статистики; – разрабатывать и использовать вероятностные и статистические модели при решении типовых прикладных задач. Владеть: – методами теории вероятностей и математической статистики.
Б1.О.05	Дискретная математика	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1 Знает основные понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов; свойства основных дискретных структур: линейных	Знать: – основные понятия и методы математической логики и теории алгоритмов; – основные понятия и методы дискретной математики. Уметь: – применять основные методы из математической логики и теории алгоритмов при решении задач; – применять основные алгоритмы и методы из теории графов и теории автоматов; – использовать полученные теоретические знания в самостоятельных исследованиях. Владеть: – методами решения прикладных задач.

			рекуррентных последовательностей, графов, конечных автоматов, комбинаторных структур; основные понятия и методы теории графов; основные понятия и методы теории конечных автоматов; основные понятия и методы комбинаторного анализа. ОПК-3.2 Умеет производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы математической логики и теории алгоритмов к решению задач математической кибернетики; решать задачи периодичности и эквивалентности для линейных рекуррентных последовательностей и конечных автоматов; применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; решать оптимизационные задачи на графах; умеет применять стандартные методы дискретной математики для решения профессиональных задач. ОПК-3.3 Владеет навыками использования языка	

			современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач; владеет навыками решения типовых комбинаторных и теоретико-графовых задач; навыками применения языка и средств дискретной математики при решении профессиональных задач.	
Б1.О.06	Дифференциальные уравнения	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1. знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных; знает основные типы обыкновенных дифференциальных уравнений и методы их решения; ОПК-3.2. умеет обосновывать основные методы дифференциального исчисления функций одной и нескольких действительных переменных;	Знать: Для достижения ОПК-3.1. Обладает знаниями основных математических понятий и методов. Для достижения ОПК-3.2. Уметь: – использовать опыт применения математических методов для решения задач профессиональной деятельности. Владеть: – владеть терминологией, основными обозначениями, принятыми в теории обыкновенных дифференциальных уравнений и ее приложениях; – владеть приемами и методами, принятыми в теории обыкновенных дифференциальных уравнений и ее приложениях; – владеть методами доказательства утверждений, принятыми в теории обыкновенных дифференциальных уравнений.
Б1.О.07	Теория информации	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и	ОПК-3.1. Знает фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации;	Знать: – фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации; – основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума; – основные методы оптимального кодирования источников

		реализовывать процедуры решения задач профессиональной деятельности	основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума; основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга); понятие пропускной способности канала связи, прямую и обратную теоремы кодирования. ОПК-3.2. Умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); решать типовые задачи кодирования и декодирования; работать с научно-технической литературой по тематике дисциплины. ОПК-3.3. Владеет основами построения математических моделей текстовой информации и моделей систем передачи информации.	информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга); – понятие пропускной способности канала связи, прямую и обратную теоремы кодирования. Уметь: – вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); – решать типовые задачи кодирования и декодирования; – работать с научно-технической литературой по тематике дисциплины. Владеть: – основами построения математических моделей текстовой информации и моделей систем передачи информации; – навыками применения математического аппарата для решения прикладных теоретико-информационных задач.
Б1.О.08	Аппаратные средства вычислительной техники	ОПК-4: Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические	ОПК-4.1. Знает архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры.	Знать: – физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники; – принципы работы и тенденции развития элементной базы, интерфейсов, процессоров и памяти, устройств ввода-вывода ЭВМ; – терминологию, уровни организации, способы классификации и стандартизации аппаратных средств вычислительной техники.

		законы и модели для решения задач профессиональной деятельности	ОПК-4.2. Умеет анализировать и синтезировать электронные схемы; определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств. ОПК-4.3. Владеет навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.	Уметь: – применять основные физические законы и модели для решения задач профессиональной деятельности; – описывать технические характеристики компонентов ЭВМ; применять программные средства диагностики ЭВМ; – собирать персональный компьютер из комплектующих. Владеть: – навыками подбора совместимых комплектующих ЭВМ, очистки и замены систем охлаждения и питания персональных компьютеров.
Б1.О.9	Физика	ОПК-4: Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Знает основные законы механики; основные законы термодинамики и молекулярной физики; основные законы электричества и магнетизма; основы теории колебаний и волн, оптики; основы квантовой физики и физики твёрдого тела. ОПК-4.2. Умеет использовать математические модели физических явлений и процессов; решать типовые прикладные физические задачи. ОПК-4.3. Владеет методами исследования физических явлений и процессов.	Знать: – базовые теоретические знания по физике; – смысл основных терминов и понятий физики; – методы и способы получения и освоения материала по физике; – о физических процессах, происходящих в окружающем мире и, в частности, о физических процессах, сопровождающих профессиональную деятельность; – основные правила оформления материалов и результатов лабораторных исследований; – правила оформления таблиц, схем, рисунков и чертежей в научных отчетах; – правила и способы вычисления погрешностей полученных данных. Уметь: – пользоваться теоретическими знания и практическими навыками, полученными в рамках изучения курса общей физики; – прогнозировать последствия физических процессов происходящих в профессиональной деятельности; – анализировать полученные экспериментальные данные. Владеть: – базовыми теоретическими знаниями и навыками лабораторных исследований в области физики; – навыком грамотного представления результатов

				исследований и навыком оформления отчетов по лабораторным работам.
Б1.О.10	Сети и системы передачи информации	ОПК-4: Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Знает основные телекоммуникационные протоколы; основные характеристики сигналов электросвязи, спектры и виды модуляции; принципы построения и функционирования систем и сетей передачи информации; способы передачи и распределения информации в телекоммуникационных системах и сетях. ОПК-4.2. Умеет пользоваться нормативными документами в области технической защиты информации; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи.	Знать: Для достижения индикатора ОПК-4.1: Знать – основные законы электричества и магнетизма; – основы теории колебаний и волн; – принципы работы элементов и функциональных узлов электронной аппаратуры; – знает архитектуру основных типов современных компьютерных систем; – структуру и принципы работы современных и перспективных микропроцессоров; – принципы работы элементов и функциональных узлов электронной аппаратуры. Уметь: Для достижения индикатора ОПК-4.2: Уметь – использовать математические модели физических явлений и процессов; – решать типовые прикладные физические задачи; – работать с современной элементной базой электронной аппаратуры; – определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств. Владеть: – методами исследования физических явлений и процессов; – навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.
Б1.О.11	Информатика	ОПК-2: Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач	ОПК-2.1 Знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере; логико-математические основы построения электронных цифровых устройств; состав, назначение аппаратных средств	Знать: – основные современные тенденции развития информатики и вычислительной техники; – организацию создания программных средств; – содержание различных этапов процесса разработки программных средств. Уметь: – работать с простейшими аппаратами, приборами и схемами, понимать принципы их действия;

		профессиональной деятельности	и программного обеспечения персонального компьютера, классификацию современных вычислительных систем, типовые структуры и принципы организации компьютерных сетей. ОПК-2.2 Умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет; составлять документы, используя прикладные программы офисного назначения. ОПК-2.3 Владеет средствами управления пользовательскими интерфейсами операционных систем.	– использовать существующие пакеты прикладных программ для решения конкретных задач. Владеть: – приемами и методами решения конкретных задач из областей технологии, с учетом требований по обеспечению информационной безопасности; – навыками работы с программно-техническими средствами; – основными принципами организации и взаимодействия программных компонентов.
Б1.О.12	Языки программирования	ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1 Знает общие принципы построения, области и особенности применения языков программирования высокого и низкого уровня; язык программирования высокого и низкого уровня (объектно-ориентированное программирование). ОПК-7.2 Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого и низкого уровня алгоритмы решения типовых профессиональных задач; ОПК-7.3 Владеет навыками разработки, документирования, тестирования и отладки	Знать: – программные средства прикладного, системного и специального назначения, современные программные комплексы; – современные средства разработки и анализа программного обеспечения на языках высокого уровня. Уметь: – выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; – использовать языки программирования для решения задач. Владеть: – навыками разработки программ на языке программирования высокого уровня; – навыками применения программных средств для решения конкретных задач;

			программ.	– навыками построения алгоритма и проведению его реализации в современных программных комплексах.
Б1.О.13	Языки Ассемблера	ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1 Знает общие принципы построения, области и особенности применения языков программирования высокого и низкого уровня; язык программирования высокого и низкого уровня (объектно-ориентированное программирование); знает язык ассемблера персонального компьютера. ОПК-7.2 Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого и низкого уровня алгоритмы решения типовых профессиональных задач; ОПК-7.3 Владеет навыками разработки, документирования, тестирования и отладки программ.	Знать: – специфику создания низкоуровневого кода под современные процессоры. – синтаксис языков ассемблера для современных процессоров. Уметь: – проектировать программное обеспечение с учётом низкоуровневой специфики архитектуры современных процессоров. – создавать код любой сложности под современные процессоры. Владеть: – навыки сопряжения низкоуровневого кода с другими программными системами. – навыками использования инструментальных средств создания кода под современные процессоры.
Б1.О.14	Системное программирование	ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации	ОПК-7.1 Знает общие принципы построения, области и особенности применения языков программирования высокого и низкого уровня; знает язык программирования высокого и низкого уровня; знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения. ОПК-7.2 Умеет работать с интегрированной средой разработки программного	Знать: – архитектуру и программный интерфейс современных операционных систем. Уметь: – создавать прикладное и системное программное обеспечение для современных операционных систем. Владеть: – навыками реализации программного обеспечения любой сложности с использованием высокоуровневых и низкоуровневых языков программирования.

		программ	обеспечения; умеет разрабатывать и реализовывать на языке высокого и низкого уровня алгоритмы решения типовых профессиональных задач; умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3 Владеет навыками разработки алгоритмов решения типовых профессиональных задач; владеет навыками разработки, документирования, тестирования и отладки программ.	
		ОПК-13: Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ОПК-13.1 Знает общие принципы построения и использования современных языков программирования высокого и низкого уровня; современные технологии программирования; показатели качества программного обеспечения; ОПК-13.2 Умеет формализовать поставленную задачу, работать с интегрированными средами разработки программного обеспечения; разрабатывать эффективные алгоритмы и программы. ОПК-13.3 Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением	Знать: – системную и программную архитектуру современных процессоров. Уметь: – создавать пользовательские программы; – создавать код режима ядра. Владеть: – навыками использования инструментальных средств создания кода под современные операционные системы.

			безопасности операционных систем распространенных семейств; навыками разработки алгоритмов для решения типовых профессиональных задач.	
Б1.О.15	Языки программирования Java	ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1 Знает общие принципы построения, области и особенности применения языков программирования высокого и низкого уровня; язык программирования высокого и низкого уровня (объектно-ориентированное программирование). ОПК-7.2 Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого и низкого уровня алгоритмы решения типовых профессиональных задач; ОПК-7.3 Владеет навыками разработки, документирования, тестирования и отладки программ.	Знать: – возможности языков программирования на примере Java; – области применения языка программирования Java; – основные особенности объектно-ориентированного подхода в программировании. Уметь: – работать в современных средствах разработки (IDE); – выделять объектную модель из поставленной задачи. Владеть: – навыками разработки программного обеспечения на языке Java.
Б1.О.16	Операционные системы	ОПК-12: Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	ОПК-12.1 Знает принципы построения современных операционных систем и особенности их применения; основные принципы конфигурирования и администрирования операционных систем. ОПК-12.2 Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и	Знать: – общее устройство принципы работы современных операционных систем (ОС); – назначение и организацию основных служебных структур данных; – принципы работы механизмов защиты операционных систем семейств Windows и Linux. Уметь: – выполнять установку, настройку, обслуживание современных ОС. Владеть: – навыками настройки учетных записей ОС.

			многопроцессорных сред с использованием средств синхронизации; применять основные методы программирования в выбранной операционной среде. ОПК-12.3 Владеет навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.	
Б1.О.17	Компьютерные сети	ОПК-15: Способен администрировать компьютерные сети и контролировать корректность их функционирования	ОПК-15.1 Знает архитектуру основных типов современных компьютерных систем; принципы построения современных операционных систем и особенности их применения; основы организации и построения компьютерных сетей; эталонную модель взаимодействия открытых систем; функции, принципы действия и алгоритмы работы сетевого оборудования. ОПК-15.2 Умеет реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования компьютерных сетей. ОПК-15.3 Владеет навыками администрирования компьютерных сетей; навыками работы с сетевым оборудованием и сетевым программным обеспечением.	Знать: – задачи и цели администрирования сетевой инфраструктуры организации; – основы функционирования сетевых протоколов и служб; – функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печати, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов; – принципы построения системы безопасности сетевой операционной системы. Уметь: – проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации; – производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы; – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности. Владеть: – технологиями и навыками построения и администрирования службы каталогов информационной системы организации; – инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования; – методами и средствами аудита и мониторинга сетевых устройств и служб.

Б1.О.18	Беспроводные сети	ОПК-15: Способен администрировать компьютерные сети и контролировать корректность их функционирования	ОПК-15.1 Знает основы организации и построения беспроводных компьютерных сетей. ОПК-15.2 Умеет реализовывать приложения для беспроводных сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования беспроводных компьютерных сетей. ОПК-15.3 Владеет навыками администрирования беспроводных компьютерных сетей; навыками работы с беспроводным сетевым оборудованием и сетевым программным обеспечением.	Знать: – задачи и цели администрирования беспроводной сетевой инфраструктуры; – основы функционирования беспроводных сетевых протоколов и служб; – принципы построения системы безопасности беспроводной сетевой инфраструктуры. Уметь: – проектировать беспроводную сетевую инфраструктуру в соответствии с потребностями построения информационной системы; – производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы; – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности. Владеть: – технологиями и навыками построения и администрирования беспроводной сетевой инфраструктуры; – методами и средствами аудита и мониторинга беспроводных сетевых устройств и служб.
Б1.О.19	Системы управления базами данных	ОПК-14: Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации	ОПК-14.1 Знает характеристики и типы систем баз данных; основные языки запросов; физическую организацию баз данных и принципы (основы) их защиты; общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в СУБД; этапы проектирования системы защиты в СУБД.	Знать: – характеристики и типы систем баз данных; – этапы проектирования баз данных; – физическую организацию баз данных; – основные модели структур данных; – способы организации файловых систем; – основные понятия о реляционной модели данных; – основные предложения языка запросов SQL; – области применения систем управления базами данных; – средства поддержания целостности в базах данных; – особенности управления данными в системах распределенной обработки; – порядок эксплуатации баз данных. Уметь: – разрабатывать программы на языках программирования четвертого поколения; – реализовывать на практике сложные структуры данных средствами реляционной СУБД;

			ОПК-14.2 Умеет проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных; настраивать и применять современные системы управления базами данных; пользоваться средствами защиты, предоставляемыми СУБД; создавать дополнительные средства защиты баз данных; проводить анализ и оценивание механизмов защиты баз данных. ОПК-14.3 Владеет методикой и навыками составления запросов для поиска информации в базах данных.	– использовать язык запросов SQL; – отображать предметную область на конкретную модель данных; – приводить в соответствие отношения при проектировании реляционной базы данных. Владеть: – навыками разработчика и администратора баз данных; – навыками поддержки и сопровождения баз данных; – навыками резервного копирования данных; – навыками обоснованного выбора инструментальных систем разработки баз данных; – навыками работы со средствами поддержания интерфейса с различными категориями пользователей СУБД; – навыками работы с системами управления базами данных на различных платформах.
Б1.О.20	Основы информационной безопасности	ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1 Знает понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. ОПК-1.2 Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта	Знать: – основные термины по проблематике информационной безопасности; – цели, задачи, принципы и основные направления обеспечения информационной безопасности; – место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; – содержание информационной войны, методы и средства ее ведения; – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Уметь: – пользоваться современной научно-технической информацией по исследуемым проблемам и задачам. Владеть: – навыками использования профессиональной

			информатизации.	терминологии в области информационной безопасности.
		ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1 Знает источники и классификацию угроз информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России. ОПК-5.2 Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.	Знать: – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь: – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Владеть: – навыками работы с нормативными правовыми актами в области информационной безопасности; – навыками применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.
Б1.О.21	Организационное и правовое обеспечение информационной безопасности	ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1 Знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы	Знать: – источники и классификацию угроз информационной безопасности; – требования по защите информации при использовании СКЗИ; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь: – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; – разрабатывать требования к системе защиты информации. Владеть: – навыками работы с нормативными правовыми актами в области информационной безопасности; – навыками применения современной нормативной базы для построения системы организационных и программно-

			организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности. ОПК-5.2 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей,предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования информационной безопасности при эксплуатации	технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.

			компьютерной системы; формулировать основные требования по защитеконфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.	
		ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1 Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем. ОПК-6.2 Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты	Знать: – нормативные правовые акты в области защиты информации. Уметь: – использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации. Владеть: – навыками обеспечения использования правовых актов в своей профессиональной деятельности.

			инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.	
Б1.О.22	Теория чисел	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1. Знает основные понятия теории чисел. ОПК-3.2. Умеет решать основные типы задач теории чисел. ОПК-3.3. Владеет навыками решения типовых линейных уравнений над полем и кольцом вычетов.	Знать: – основные понятия, связанные с теорией делимости, сравнениями и кольцами классов вычетов и их свойства; – формулировку основных результатов по этим темам. Уметь: – ориентироваться в соотношении между собой понятий теории чисел; – доказать свойства основных понятий курса; – доказать основные теоретические результаты, приводимые в курсе теории чисел. Владеть: – основами теории чисел; – теоретической базой, связанной с теорией делимости, сравнениями и кольцами классов вычетов; – теоретической базой, связанной с базовыми приложениями теории чисел в криптографии.
Б1.О.23	Модели безопасности компьютерных систем	ОПК-8: Способен применять методы научных исследований при	ОПК-8.1 Знает основные методы научных исследований при разработке моделей безопасности компьютерных	Знать: – виды и состав угроз информационной безопасности; – принципы и общие методы обеспечения информационной безопасности;

		проведении разработок в области обеспечения безопасности компьютерных систем и сетей	систем. ОПК-8.2 Умеет применять методы научных исследований при проведении разработок моделей безопасности компьютерных систем. ОПК-8.3 Владеет способами моделирования безопасности компьютерных систем.	– источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; – каналы и методы несанкционированного доступа к конфиденциальной информации; – состав объектов защиты информации. Уметь: – определять состав конфиденциальной информации; – определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию; – определять возможные каналы и методы несанкционированного доступа; – принимать решения при выборе средств защиты информации на основе анализа угроз и рисков; – организовывать системное обеспечение защиты информации. Владеть: – навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий; – навыками разработки основных политик безопасности; – критериями, условиями и принципами отнесения информации к защищаемой; – методологией построения систем защиты автоматизированных систем.
		ОПК-11: Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	ОПК-11.1 Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности	Знать: – типовые модели политик безопасности КС, политик управления доступом и информационными потоками. Уметь: – самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности, управления доступом и информационными потоками, с учетом заданных требований. Владеть: – методами разработки моделей политик безопасности, управления доступом и информационными потоками.

			информационных потоков. ОПК-11.2 Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками. ОПК-11.3 Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	
Б1.О.24	Методы и средства криптографической защиты информации	ОПК-10: Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Знает основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты. ОПК-10.2 Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов. ОПК-10.3 Владеет навыками использования типовых криптографических алгоритмов.	Знать: – основные понятия и классификацию средств криптографической защиты информации; – различия между стеганографией и криптографией; – основные методы симметричного шифрования; – классификацию методов симметричного шифрования; – основные свойства симметричных криптосистем; – понятие хеш-функции; – основные понятия, основные алгоритмы электронной цифровой подписи; – основные стандарты на алгоритмы цифровой подписи; – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. Уметь: – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и распределения ключей;

				– проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – основными методами симметричного шифрования; алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.
Б1.О.25	Криптографические протоколы	ОПК-10: Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Знает типовые криптопротоколы, используемые в сетях связи; основные типы криптопротоколов и принципов их построения с использованием шифрсистем. ОПК-10.2 Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. ОПК-10.3 Владеет подходами к разработке и анализу безопасности криптографических протоколов.	Знать: – различия между стеганографией и криптографией; – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. Уметь: – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – основными методами симметричного шифрования; алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем;

				методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.
Б1.О.26	Основы построения защищенных компьютерных сетей	ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.1 Знает методы защиты и средства обеспечения безопасности в операционных системах, компьютерных сетях и системах управления базами данных; методы предотвращения и обнаружения вторжений в операционных системах, компьютерных сетях и системах управления базами данных. ОПК-9.2 Умеет осуществлять меры противодействия нарушениям безопасности в операционных системах, компьютерных сетях и системах управления базами данных с использованием различных программных и аппаратных средств защиты.	Знать: – иметь представление о построения современной системы защиты вычислительной сети предприятия; – знать основы средств и методов реализации атак на сетевые ресурсы; – знать основы принципов использования межсетевых экранов (МЭ); – знать основы построения систем адаптивной безопасности в вычислительных сетях; – знать основы построения виртуальных частных сетей; – стандарты по оценке защищенных сетевых систем и их теоретические основы; методы и средства проектирования, реализации и оценки защищенных сетевых систем. Уметь: – строить системы адаптивной безопасности в вычислительных сетях; – применять стандарты по оценке защищенных сетевых систем при анализе и проектировании систем защиты информации. Владеть: – навыком работы построения систем адаптивной безопасности в вычислительных сетях; – навыком работы построением виртуальных частных сетей; – методами анализа сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности.
		ОПК-16: Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных	ОПК-16.1 Знает средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети;	Знать: – угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем; – типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем; – условия их осуществимости, возможные последствия, способы предотвращения. Уметь:

		системах и сетях	защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений. ОПК-16.2 Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. ОПК-16.3 Владеет навыками настройки межсетевых экранов.	– устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владеть: – навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в сетях.
Б1.О.27	Основы построения защищенных баз данных	ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации	ОПК-9.1 Знает методы защиты и средства обеспечения безопасности в операционных системах, компьютерных сетях и системах управления базами данных; методы предотвращения и обнаружения вторжений в операционных системах, компьютерных сетях и системах управления базами данных. ОПК-9.2 Умеет осуществлять меры противодействия нарушениям безопасности в операционных системах, компьютерных сетях и системах управления базами данных с	Знать: – программно-аппаратные средства обеспечения информационной безопасности в типовых операционных систем в системах управления базами данных (БД), вычислительных сетях; – основные определения и положения безопасности БД; – основные защитные механизмы БД. Уметь: – применять программно-аппаратных средств защиты информации для обеспечения безопасности БД; – оценивать угрозы безопасности клиентским ОС осуществлять проверку защищенности БД; – осуществлять рациональный выбор средств и методов защиты информации в БД. Владеть: – навыками администрирования прав пользователей и

		от утечки по техническим каналам, сетей и систем передачи информации	использованием различных программных и аппаратных средств защиты.	аудита доступа к ресурсам БД; – навыками настройки политики безопасности и учетных записей БД; – навыками администрирования протокольных средств обеспечения безопасности БД.
		ОПК-16: Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	ОПК-16.1 Знает общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в СУБД; этапы проектирования системы защиты в СУБД. ОПК-16.2 Умеет пользоваться средствами защиты, предоставляемыми СУБД; создавать дополнительные средства защиты баз данных; проводить анализ и оценивание механизмов защиты баз данных. ОПК-16.3. Владеет методикой и навыками использования средств защиты, предоставляемых СУБД.	Знать: – угрозы и методы нарушения информационной безопасности БД; – типовые модели атак, направленных на преодоление защиты БД; – условия их осуществимости, возможные последствия, способы предотвращения. Уметь: – устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем, БД. Владеть: – навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в БД.
Б1.О.28	Защита информации от утечки по техническим каналам	ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в	ОПК-6.1. Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и	Знать: Для достижения индикатора ОПК-6.1: Знать систему нормативных правовых актов и стандартов по лицензированию в области технической защиты конфиденциальной информации; основные угрозы безопасности информации и модели нарушителя компьютерных систем Уметь: Для достижения индикатора ОПК-6.2: Уметь разрабатывать

		соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем. ОПК-6.2. Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и	модели угроз и модели нарушителя компьютерных систем; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы. Владеть: Для достижения индикатора ОПК-6.2: Владеть навыками защиты информации от утечки по техническим каналам

			оценивания защищенности компьютерной системы.	
		ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.1. Знает технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; возможности технических средств перехвата информации. ОПК-9.2. Умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации. ОПК-9.3. Владеет методами и средствами технической защиты информации.	Знать: Для достижения индикатора ОПК-9.1: Знать технические каналы утечки информации; возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; основные характеристики сигналов электросвязи, спектры и виды модуляции; принципы построения и функционирования систем и сетей передачи информации; способы передачи и распределения информации в телекоммуникационных системах и сетях; основные телекоммуникационные протоколы. Уметь: Для достижения индикатора ОПК-9.2: Уметь пользоваться нормативными документами в области технической защиты информации; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи. Владеть: Для достижения индикатора ОПК-9.3: Владеть навыками решения задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации
Б1.О.29	Защита в операционных системах	ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами	ОПК-9.1 Знает методы защиты и средства обеспечения безопасности в операционных системах, компьютерных сетях и системах управления базами данных; методы предотвращения и обнаружения вторжений в операционных системах, компьютерных сетях и системах управления базами данных. ОПК-9.2 Умеет осуществлять меры противодействия нарушениям безопасности в	Знать: – основные понятия операционных систем и их защиты; – основные понятия, основные алгоритмы хранения и обработки данных ОС; – основные стандарты и алгоритмы передачи данных; – основные понятия защищенных операционных систем, баз данных и компьютерных сетей; – основные актуальные модели атак; – понятие защиты информации, системы защиты; – аппаратно-программные средства защиты информации: – средства обеспечения конфиденциальности данных; – средства аутентификации электронных данных и средства управления ключевой информацией;

		данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	операционных системах, компьютерных сетях и системах управления базами данных с использованием различных программных и аппаратных средств защиты.	– цели и концептуальные основы защиты информации; – основные виды угроз безопасности информации и их классификацию. Уметь: – осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации; – оценивать угрозы безопасности клиентским ОС осуществлять проверку защищенности клиентских ОС; – осуществлять проверку защищенности серверных ОС; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – навыками настройки политики безопасности и учетных записей ОС оценки степени защищенности клиентских ОС; – навыками оценки степени безопасности ОС; – навыками администрирования протокольных средств обеспечения безопасности ОС; – навыками администрирования прав пользователей и аудита доступа к ресурсам ОС; – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети интернет.

		ОПК-13: Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ОПК-13.1 Знает средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем. ОПК-13.2 Умеет формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем. ОПК-13.3 Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.	Знать: – цели и концептуальные основы защиты информации; – основные виды угроз безопасности информации и их классификацию; – программно-аппаратные средства защиты информации: – средства обеспечения конфиденциальности данных; – средства аутентификации электронных данных и средства управления ключевой информацией; – требования к криптографическим системам защиты информации; – понятие и виды криптографических атак. Уметь: – оценивать угрозы безопасности клиентским ОС; – проектировать и использовать системы электронной цифровой подписи; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем; – использовать алгоритмы генерации, хранения и распределения ключей; – осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации; – осуществлять проверку защищенности клиентских ОС; – осуществлять проверку защищенности серверных ОС. Владеть: – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети интернет.
Б1.О.30	Защита программ и данных	ОПК-13.Способен разрабатывать	ОПК-13.1. знает основные средства и методы защиты	Знать: – особенности программирования шеллкодов;

		компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	программного обеспечения от анализа; знает основные типы уязвимостей программного обеспечения; ОПК-13.2. умеет использовать программные средства анализа защиты компьютерных систем; умеет разрабатывать компоненты средств защиты информации.	– методы исследования программного обеспечения без исходных кодов. Уметь: – создавать шеллкоды для современных операционных системы под разные аппаратные платформы; – исследовать программное обеспечение без исходных кодов. Владеть: – навыками создания шеллкодов с учетом специфики различных сценариев использования; – навыками использования современных средств исследования программного обеспечения без исходных кодов.
		ОПК-16.Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	ОПК-16.1. знает средства мониторинга работоспособности средств защиты информации в компьютерных системах и сетях ОПК-16.2. знает методики анализа эффективности средств защиты информации в компьютерных системах и сетях умеет использовать средства мониторинга работоспособности средств защиты информации в компьютерных системах и сетях.	Знать: – базовые методы функционирования вредоносного программного обеспечения; – методы защиты программного обеспечения от исследования, копирования, модификации. Уметь: – реализовывать базовые функциональные компоненты вредоносного программного обеспечения; – реализовывать методы защиты программного обеспечения от исследования с учетом специфики операционных систем, аппаратной платформы, используемой архитектуры. Владеть: – навыками исследования вредоносного программного обеспечения с использованием современных инструментов анализа и собственных утилит; – навыками реализации методов защиты программного обеспечения от исследования и обхода этих методов.
Б1.О.31.	Введение в специальность	ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном	ОПК-1.1. Знает понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной	Знать: – понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

		обществе, их значение для обеспечения объективных потребностей личности, общества и государства	информационной политики; знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; ОПК-1.2. Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.	Уметь: – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Владеть: – навыками построения систем защиты информации.
		ПК-1: Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов. ПК-1.2. Демонстрирует умения: применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа. ПК-1.3. Имеет практический опыт (навыки): составления экспертного заключения.	Знать: – свойства защищаемой информации, основы технологий поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов. Уметь: – предложить простейшие механизмы защиты от базовых угроз информационно безопасности; – применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа. Владеть: – навыками составления экспертного заключения.
				Знать: – перечень базовых угроз информационной безопасности. Уметь: – определять основные пути реализации угроз информационной безопасности. Владеть: – навыками реализации простейших атак на базы данных и симметричные шифры.
Дисциплины(модули) специализации				
Б1.О.32.01	Основы компьютерной	ОПК-6.3.: Способен в качестве	ОПК-6.3.1.знает порядок проведения экспертизы	Знать: – порядок проведения экспертизы вычислительной техники

	криминалистики	привлекаемого эксперта при проведении следственных и судебных действий применять нормативные правовые акты, методические документы, основы компьютерной криминалистики	вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов; знает виды преступлений в сфере компьютерной информации; знает основные требования, предъявляемые к составу и оформлению научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; знает методику проведения работ по информационно-аналитической и технической экспертизе компьютерных систем. ОПК-6.3.2.Умеет подготавливать научно-технические экспертные заключения, по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; умеет обобщать и анализировать данные, получаемые в ходе проведения работ по информационно-аналитической и технической экспертизе компьютерных систем; фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов; умеет фиксировать и	и носителей компьютерной информации с учетом нормативных правовых актов; – виды преступлений в сфере компьютерной информации; – основные требования, предъявляемые к составу и оформлению научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; – методику проведения работ по информационно-аналитической и технической экспертизе компьютерных систем. Уметь: – подготавливать научно-технические экспертные заключения, по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; – обобщать и анализировать данные, получаемые в ходе проведения работ по информационно-аналитической и технической экспертизе компьютерных систем; фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов; – фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов. Владеть: – навыками самостоятельного проведения компьютерно-технических экспертиз и исследований.

			документировать следы компьютерных преступлений, правонарушений и инцидентов.	
Б1.О.32.02	Экспертиза вычислительной техники и компьютерных носителей информации	ОПК-6.2.: Способен проводить экспертные исследования вычислительной техники и компьютерных носителей информации в рамках информационно-аналитической и технической экспертизы компьютерных систем	ОПК-6.2.1.Знает нормативные и правовые акты, регламентирующие проведение компьютерно-технических экспертиз; знает современные методы и средства проведения экспертиз вычислительной техники и носителей компьютерной информации; знает основные типы экспертиз вычислительной техники и носителей компьютерной информации; знает классификацию свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы; знает форматы хранения информации в анализируемой компьютерной системе. ОПК-6.2.2.Умеет обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации; умеет определять свойства аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния; умеет анализировать структуру механизма изменения свойств (эксплуатационных режимов) аппаратных средств в составе	Знать: – нормативные и правовые акты, регламентирующие проведение компьютерно-технических экспертиз; – современные методы и средства проведения экспертиз вычислительной техники и носителей компьютерной информации; – основные типы экспертиз вычислительной техники и носителей компьютерной информации; – классификацию свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы; – форматы хранения информации в анализируемой компьютерной системе. Уметь: – обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации; – определять свойства аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния; – анализировать структуру механизма изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы. Владеть: – навыками выполнения компьютерных экспертиз и исследований.

			компьютерной системы.	
Б1.О.32.03	Технологии выявления следов компьютерных преступлений, правонарушений и инцидентов	ОПК-6.1.: Способен использовать технологии поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов;	ОПК-6.1.1.Знает основные этапы и методы проведения расследования компьютерных преступлений, правонарушений и инцидентов; знает методы и средства сбора и обращения с доказательными данными. ОПК-6.1.2.Умеет определять причины, цели и условия изменения свойств (состояния) программного обеспечения; умеет обращаться со свободно распространяемыми инструментальными средствами сбора, анализа и хранения доказательных данных.	Знать: – основные этапы и методы проведения расследования компьютерных преступлений, правонарушений и инцидентов; – методы и средства сбора и обращения с доказательными данными. Уметь: – определять причины, цели и условия изменения свойств (состояния) программного обеспечения; – обращаться со свободно распространяемыми инструментальными средствами сбора, анализа и хранения доказательных данных. Владеть: – способами правильного установления, фиксации и оценки следов компьютерных преступлений и инцидентов.
Часть, формируемая участниками образовательных отношений				
Б1.В.01	Тестирование компьютерных систем на проникновения	ПК-2: Способен проводить мониторинг защищенности компьютерных систем	ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации.	Знать: – этапы проведения тестирования компьютерных систем на проникновение; – теоретические основы компьютерных атак, моделируемых в рамках проведения экспериментов по проникновению в компьютерные системы; – принципы работы сканеров безопасности и методику проверки получаемых ими сведений; – правила документирования и построения отчетов по результатам проводимых тестов на проникновение. Уметь: – использовать сканеры информационной безопасности и проводить оценку, получаемых ими сведений; – моделировать современные компьютерные атаки, представляющие актуальные угрозы информационной безопасности для компьютерных систем; – детектировать средства обнаружения компьютерных вторжений и предотвращения утечек информации; – использовать приемы обхода IDS, IPS, DLP-систем, антивирусного программного обеспечения и

			ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет. ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.	криптографических протоколов, применяемых для защиты компьютерных систем; – проводить оценку конфигурации средств защиты информации и давать рекомендации по ее корректировке. Владеть: – практическими навыками проведения тестирования компьютерных систем на проникновение и подготовки по их результатам соответствующих отчетов.
Б1.В.02	Методы и стандарты оценки защищенности компьютерных систем	ПК-3: Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности	Знать: – российские и зарубежные стандарты в области информационной безопасности; – современные критерии и стандарты для анализа безопасности компьютерных систем. Уметь: – оценивать соответствие проектной и эксплуатационной документации информационной системы на соответствие стандарту в области информационной безопасности; – применять современные критерии и стандарты для анализа безопасности компьютерных систем. Владеть: – практическими навыками оценки защищенности на

			существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.	соответствие стандартам информационной безопасности ЦБ РФ в области информационных систем, функционирующих в финансовой сфере; – практическими навыками работы с современными критериями и стандартами для анализа безопасности компьютерных систем.
Б1.В.03	Методы верификации	ПК-3: Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости	Знать: – основы построения и реализации биометрических систем аутентификации, – основы тестирования и оценки надежности разработанных биометрических систем аутентификации. Уметь: – самостоятельно строить и анализировать алгоритмы, которые используются для построения биометрических систем аутентификации. Владеть: – навыками построения алгоритмов для биометрических систем аутентификации и проведения тестирования разработанных алгоритмов.

			компьютерных систем.	
Б1.В.ДВ.01 Элективные дисциплины (модули) 1				
Б1.В.ДВ.01.01	Защита IoT сетей	ПК-2: Способен проводить мониторинг защищенности компьютерных систем	ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет. ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров	Знать: – общие положения интернета вещей; – стандарты и протоколы передачи данных в IoT; – практическую реализацию IoT; – принципы построения систем обнаружения компьютерных атак; – актуальные методы обработки данных мониторинга безопасности компьютерных систем и сетей; – нормативные правовые акты в области защиты информации. Уметь: – решать задачу управления безопасностью компьютерных систем; – применять инструментальные средства проведения мониторинга защищенности компьютерных систем; – применять методы анализа защищенности компьютерных систем и сетей; – структурировать аналитическую информацию для включения в отчет. Владеть: – навыками практической реализации IoT; – навыками анализа защищенности компьютерных систем с использованием сканеров безопасности; – навыками анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; – навыками составления отчетов по результатам проверок.

			безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.	
Б1.В.ДВ.01.02	Сетевые технологии	ПК-2: Способен проводить мониторинг защищенности компьютерных систем	ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать	Знать: – архитектуру MPLS VPN; – базовые концепции MPLS; – модели Overlay VPN и Peer-to-Peer VPN; – назначение и распределение меток в сети MPLS; – основные концепции проектирования компьютерных сетей; – основы построения вычислительных сетей предприятия; – основы функционирования сетевых протоколов и служб; – понятие инфраструктуры корпоративной сети; – понятия и технологии корпоративных сетей, сетей LAN, сетей WAN; – принципы адресации и коммутации в корпоративной сети; – принципы использования IP-адресации в проекте компьютерной сети; – принципы построения системы безопасности сетевой операционной системы; – терминологию и архитектуру MPLS; – функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печа-ти, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов; – эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы. Уметь: – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности; – внедрять списки доступа, позволяющие разрешать или отклонять трафик определенного типа; – настраивать протоколы маршрутизации устройств Cisco; – настраивать фильтрацию трафика с использованием

			аналитическую информацию для включения в отчет. ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.	списков контроля доступа; – описывать существующую компьютерную сеть, определять требования (влияние используемых приложений, требования пользователей, технические параметры и др.); – проводить испытания на прототипе сети WAN и устранять неполадки в корпоративных сетях; – проектировать простую компьютерную сеть с использованием технологий Cisco (разрабатывать схему IP-адресации, соответствующую требованиям локальной компьютерной сети; составлять список оборудования, соответствующего требованиям проекта локальной компьютерной сети; получать и обновлять программное обеспечение Cisco IOS для устройств Cisco); – получать и обновлять программное обеспечение Cisco IOS для устройств Cisco); – проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации; – производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы; – работать с протоколом VTP; – работать с протоколом связующего дерева STP; – разрабатывать и конфигурировать MPLS VPN; – разрабатывать технические и коммерческие предложения по созданию и модернизации компьютерной сети для комплекса зданий; – создавать каналы в корпоративной сети WAN; – создавать локальную сеть в соответствии с утвержденным проектом: настраивать коммутатор с поддержкой технологии VLAN и соединений между коммутаторами. Владеть: – инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования; – методами и средствами аудита и мониторинга сетевых устройств и служб; – методикой анализа сетевого трафика; – навыками анализа требований заказчика и проектирования

				компьютерной сети; – навыками анализа, проектирования и настройки схем потоков трафика в компьютерной сети; – навыками мониторинга работы сети, обследования и модернизации сетевого оборудования; – навыками настройки коммутации в корпоративной сети; – навыками настройки адресации в сети на базе технологий VLSM, NAT и PAT; – навыками настройки механизмов фильтрации трафика на базе списков контроля доступа (ACL); – навыками настройки протоколов маршрутизации на базе протоколов RIPv2, EIGRP, OSPF; – навыками определения влияния приложений на проект сети; – навыками оценки качества и соответствия требованиям проекта сети; – навыками работы с виртуальными сетями VLAN; – навыками создания и настройки каналов корпоративной сети на базе технологий PPP, PAP, CHAP и Frame Relay; – навыками устранения проблем коммутации, связи, маршрутизации и конфигурации WAN; – навыками фильтрации, контроля и обеспечения безопасности сетевого трафика; – технологиями и навыками построения и администрирования службы каталогов информационной системы организации.
Б1.В.ДВ.02 Элективные дисциплины (модули) 2				
Б1.В.ДВ.02.01	Дополнительные главы криптографии	ПК-3: Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а	Знать: – роль эллиптических кривых в современных асимметричных шифрах; – формальные требования, предъявляемые к криптографическим эллиптическим кривым. Уметь: – анализировать криптографические эллиптические кривые на предмет их защищённости; – конструировать эллиптические кривые, обладающие заданными свойствами. Владеть: – навыками разработки и конфигурирования программно-

			также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.	аппаратных средств криптографической защиты информации, основанных на криптографических эллиптических кривых.
Б1.В.ДВ.02.02	Исследование вредоносного программного обеспечения	ПК-3: Способен проводить анализ безопасности компьютерных систем	ПК-3.1 Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2 Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3 Имеет практический опыт (навыки): выполнение	Знать: – методы проникновения в компьютерные системы, используемые современным вредоносным программным обеспечением; – методы функционирования современного вредоносного программного обеспечения. Уметь: – реализовывать современные атаки на компьютерные системы; – исследовать вредоносное программное обеспечение. Владеть: – инструментами проведения современных атак на компьютерные системы; – навыками использования инструментальных средств исследования вредоносного программного обеспечения.

			анализа уязвимости компьютерных систем.	
Комплексные модули				
К.М.01 Системное и критическое мышление				
К.М.01.01	Философия	УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Критически анализирует проблемную ситуацию с целью выработки стратегии действий, аргументировано формулирует собственные суждения и оценки. УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения проблемной ситуации.	Знать: – основные положения теории систем, функциональных систем и генетических, саморазвивающихся систем. Уметь: – осуществлять поиск, критический анализ проблемных ситуаций на основе системного подхода, – вырабатывать стратегию действий. Владеть: – способами поиска и критического анализа проблемных ситуаций на основе системного подхода, – способами разработки стратегии действий.
К.М.01.02	Сбор данных из открытых источников (научный семинар)	УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Критически анализирует проблемную ситуацию с целью выработки стратегии действий, аргументировано формулирует собственные суждения и оценки. УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения проблемной ситуации.	Знать: – основы выполнения эффективного поиска информации. Уметь: – определять критерии системного анализа для поставленных задач. Владеть: – навыками системного анализа и поиска информации.
		ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария	ОПК-7.2.3 умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач; ОПК-7.3.2 владеет навыками разработки алгоритмов решения типовых профессиональных задач	Знать: – информационные модели знаний, методы представления инженерии, формализации, автоформализации и представления знаний; – математические модели представления знаний, методы работы со знаниями. Уметь: – разрабатывать модели и методы исследования предметных областей; – применять методы представления и обработки знаний в прикладных задачах защиты информации. Владеть: – способами работы с базами данных и базами знаний;

		программирования и способов организации программ		– базовыми принципами и методологией построения информационных систем как систем, основанных на знаниях.
К.М.01.03	Теоретико-числовые методы в криптографии	УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Критически анализирует проблемную ситуацию с целью выработки стратегии действий, аргументировано формулирует собственные суждения и оценки. УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения проблемной ситуации.	Знать: – основы выполнения эффективного поиска информации. Уметь: – определять критерии системного анализа для поставленных задач. Владеть: – навыками системного анализа и поиска информации.
		ОПК-10: Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; базовые понятия теории эллиптических кривых. ОПК-10.2 Умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях; исследовать и решать сравнения в кольцах вычетов; использовать достаточные условия простоты для построения больших простых чисел; оценивать теоретическую сложность применяемых алгоритмов. ОПК-10.3 Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах	Знать: – точные и асимптотические оценки сложности основных теоретико-числовых алгоритмов; – основные теоретико-числовые методы и подходы для решения прикладных задач. Уметь: – применять основные теоретико-числовые результаты, изучаемые в курсе, для решения задач в криптографии. Владеть: – основными теоретико-числовыми методами, которые используются или могут использоваться в криптографии.

			многочленов; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.	
К.М.01.04	Искусственный интеллект (научный семинар)	УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Критически анализирует проблемную ситуацию с целью выработки стратегии действий, аргументировано формулирует собственные суждения и оценки. УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения проблемной ситуации.	Знать: – основы выполнения эффективного поиска информации. Уметь: – определять критерии системного анализа для поставленных задач. Владеть: – навыками системного анализа и поиска информации.
		ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1 Знает общие принципы построения, области и особенности применения языков программирования высокого уровня; язык программирования высокого уровня. ОПК-7.2 Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач. ОПК-7.3 Владеет навыками разработки, документирования, тестирования и отладки программ; навыками разработки алгоритмов решения типовых профессиональных задач.	Знать: – подходы и технику решения задач искусственного интеллекта; – информационные модели знаний, методы представления инженерии, формализации, автоформализации и представления знаний; – математические модели представления знаний, методы работы со знаниями. Уметь: – разрабатывать модели и методы исследования предметных областей, строить нечеткие модели для прикладных задач; – применять методы представления и обработки знаний в прикладных задачах защиты информации. Владеть: – способами работы с базами данных и базами знаний; – базовыми принципами и методологией построения информационных систем как систем, основанных на знаниях.
		ОПК-8: Способен применять методы научных исследований при	ОПК-8.1 Знает основные понятия и определения, используемые при описании моделей безопасности	Знать: – типовые модели политик безопасности компьютерных систем, политик управления доступом и информационными потоками.

		проведении разработок в области обеспечения безопасности компьютерных систем и сетей	компьютерных систем; средства и методы хранения и передачи и анализа конфиденциальной информации. ОПК-8.2 Умеет разрабатывать модели обнаружения угроз и модели обнаружения нарушителя безопасности компьютерных систем.	Уметь: – самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности, управления доступом и информационными потоками, с учетом заданных требований. Владеть: – методами разработки моделей политик безопасности, управления доступом и информационными потоками.
К.М.01.05	Нечеткие модели и их приложения	УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Выполняет поиск информации, определяет критерии системного анализа поставленных задач УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения поставленных задач	Знать: Для достижения УК 1.1: знать область применения теории нечетких множеств при проведении критического анализа проблемных ситуация на основе системного подхода Уметь: Для достижения УК 1.2. уметь проводить анализ проблемных ситуация с привлечением аппарата нечетких множеств Владеть: Для достижения УК 1.1: владеть навыками разработки алгоритмов управления системами на основе правил нечеткого вывода
		ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1. Знает основы теории нечетких множеств ОПК-3.2. Умеет использовать методы на основе теории нечетких множеств для решения прикладных задач ОПК-3.3. Владеет навыками применения алгоритмов управления системами на основе правил нечеткого вывода	Знать: Для достижения ОПК 3.1: знать основные методы нечеткого математического моделирования Уметь: Для достижения ОПК 3.2: уметь применять математические методы на основе теории нечетких множеств Владеть: Для достижения ОПК 3.3: владеть навыками разработки и реализации процедуры решения прикладных задач на основании совокупности методов теории нечетких множеств
К.М.02 Управление проектами				
К.М.02.01	Правоведение	УК-1: Способен осуществлять критический анализ проблемных ситуаций	УК-1.1. Критически анализирует проблемную ситуацию с целью выработки стратегии действий, аргументировано формулирует	Знать: – основы права и законодательства России; – основы конституционного строя Российской Федерации; – характеристику основных отраслей российского права;

		на основе системного подхода, вырабатывать стратегию действий	собственные суждения и оценки. УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения проблемной ситуации.	– обстоятельства, при которых происходит зарождение, развитие и прекращение правовых отношений; – ограничения и запреты, установленный правовыми нормами Уметь: – применять основы правовых знаний в различных сферах жизнедеятельности; – отграничивать правомерное поведение от противоправного; – соблюдать нормы законодательства; – анализировать основные правовые акты; – отличать обстоятельства, отягчающие или смягчающие ответственность; – определять круг задач в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений Владеть: – навыками использования основ правовых знаний в различных сферах жизнедеятельности; – навыками соблюдения норм законодательства; – анализировать основные правовые акты; – различать виды правоотношений и характерные для них объекты правоотношений; – определения круга задач в рамках поставленной цели и выбора оптимальных способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.
		УК-10: Способен формировать нетерпимое отношение к проявлению экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной	УК-10.1. Имеет представление о содержании понятий «экстремизм», «терроризм», основных формах их проявления и последствиях. УК-10.2. Имеет представление о содержании понятия «коррупционное поведение», разграничивает коррупционные и схожие некоррупционные явления в различных сферах жизни общества.	Знать: – понятие коррупции, коррупционного поведения; –положения антикоррупционного законодательства. Уметь: – применять нормы антикоррупционного законодательства. Владеть: – навыками применения норм антикоррупционного законодательства.

		деятельности	УК-10.3. Организует профессиональную среду, опираясь на этические и правовые нормы поведения, препятствующие проявлениям экстремизма, терроризма, формированию коррупционного поведения.	
К.М.02.02	Экономика	УК-9: Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1. Понимает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике. УК-9.2. Применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски.	Знать: – основные экономические категории и законы, принципы и методы экономического анализа. Уметь: – интерпретировать содержание социально-экономических процессов с точки зрения личных, коллективных и общественных интересов. Владеть: – способностью использовать экономические знания для принятия обоснованных экономических решений в различных областях жизнедеятельности.
К.М.02.03	Языки программирования Python	УК-2: Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает последовательность их реализации. УК-2.2. Формулирует проблему, на решение которой направлен проект, грамотно определяет цель проекта. УК-2.3. Проектирует решение конкретных задач проекта, выбирая оптимальный способ их решения.	Знать: – нормативно-правовую базу, регулирующую деятельность по управлению проектами. Уметь: – грамотно формулировать цель проекта; – исходя из сформулированной цели определять конкретные задачи для реализации поставленной цели. Владеть: – навыками выбора оптимального решения поставленной проблемы и достижения заявленной цели.
		ОПК-7: Способен создавать программы	ОПК-7.1 Знает общие принципы построения, области и	Знать: – информационные модели знаний, методы представления

		на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	особенности применения языков программирования высокого и низкого уровня; язык программирования высокого и низкого уровня (объектно-ориентированное программирование). ОПК-7.2 Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого и низкого уровня алгоритмы решения типовых профессиональных задач; ОПК-7.3 Владеет навыками разработки, документирования, тестирования и отладки программ.	инженерии, формализации, автоформализации и представления знаний; – математические модели представления знаний, методы работы со знаниями. Уметь: – разрабатывать модели и методы исследования предметных областей; – применять методы представления и обработки знаний в прикладных задачах защиты информации. Владеть: – способами работы с базами данных и базами знаний; – базовыми принципами и методологией построения информационных систем как систем, основанных на знаниях.
К.М.02.04	Параллельное программирование	УК-2: Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает последовательность их реализации. УК-2.2. Формулирует проблему, на решение которой направлен проект, грамотно определяет цель проекта. УК-2.3. Проектирует решение конкретных задач проекта, выбирая оптимальный способ их решения.	Знать: – нормативно-правовую базу, регулирующую деятельность по управлению проектами. Уметь: – грамотно формулировать цель проекта; – исходя из сформулированной цели определять конкретные задачи для реализации поставленной цели. Владеть: – навыками выбора оптимального решения поставленной проблемы и достижения заявленной цели.
		ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства	ОПК-7.1 Знает общие принципы построения, области и особенности применения языков программирования высокого уровня; знает язык программирования высокого уровня (объектно-	Знать: – современные языки и системы программирования; – программные средства прикладного, системного и специального назначения, современные программные комплексы. Уметь: – использовать языки программирования для решения

		программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ориентированное программирование); знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения; ОПК-7.2 Умеет работать с интегрированной средой разработки программного обеспечения; умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач; умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3 Владеет навыками разработки алгоритмов решения типовых профессиональных задач; владеет навыками разработки, документирования, тестирования и отладки программ.	различных профессиональных задач. Владеть: – навыками использования систем программирования, инструментальных средств для решения профессиональных задач; – навыками применения программных средств для решения конкретных задач; – навыками построения алгоритма и проведению его реализации в современных программных комплексах.
К.М.02.05	Методы программирования	УК-2: Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает последовательность их реализации. УК-2.2. Формулирует проблему, на решение которой направлен проект, грамотно определяет цель проекта. УК-2.3. Проектирует решение конкретных задач проекта, выбирая оптимальный способ их решения.	Знать: – нормативно-правовую базу, регулирующую деятельность по управлению проектами. Уметь: – грамотно формулировать цель проекта; – исходя из сформулированной цели определять конкретные задачи для реализации поставленной цели. Владеть: – навыками выбора оптимального решения поставленной проблемы и достижения заявленной цели.

		ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1 Знает базовые структуры данных; основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения. ОПК-7.2 Умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3 Владеет навыками разработки алгоритмов решения типовых профессиональных задач.	Знать: – возможности современных языков программирования на примере C++; – способы математического описания алгоритмов; – подходы к разработке алгоритмов в области системного и прикладного программного обеспечения; – набор фундаментальных алгоритмов решения прикладных задач различного характера. Уметь: – использовать современные интегрированные среды разработки; – составить математическую модель алгоритма; – кодировать алгоритмы на языках высокого уровня. Владеть: – навыками построения безопасного и эффективного кода; – математическими способами анализа алгоритмов.
К.М.02.06	Web-программирование	УК-2: Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает последовательность их реализации. УК-2.2. Формулирует проблему, на решение которой направлен проект, грамотно определяет цель проекта. УК-2.3. Проектирует решение конкретных задач проекта, выбирая оптимальный способ их решения.	Знать: – нормативно-правовую базу, регулирующую деятельность по управлению проектами. Уметь: – грамотно формулировать цель проекта; – исходя из сформулированной цели определять конкретные задачи для реализации поставленной цели. Владеть: – навыками выбора оптимального решения поставленной проблемы и достижения заявленной цели.
		ОПК-7: Способен создавать программы на языках высокого и	ОПК-7.1 Знает общие принципы построения, области и особенности применения языков	Знать: – программные средства прикладного, системного и специального назначения, современные программные

		низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	программирования высокого уровня. ОПК-7.2 Умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач. ОПК-7.3 Владеет навыками разработки алгоритмов решения типовых профессиональных задач, документирования, тестирования и отладки программ.	комплексы. Уметь: – использовать языки программирования для решения задач. Владеть: – навыками применения программных средств для решения конкретных задач; – навыками построения алгоритма и проведению его реализации в современных программных комплексах; – навыками использования профессиональной терминологии в области web-программирования.
К.М.02.07	Технологии программирования	УК-2: Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает последовательность их реализации. УК-2.2. Формулирует проблему, на решение которой направлен проект, грамотно определяет цель проекта. УК-2.3. Проектирует решение конкретных задач проекта, выбирая оптимальный способ их решения.	Знать: – нормативно-правовую базу, регулирующую деятельность по управлению проектами. Уметь: – грамотно формулировать цель проекта; – исходя из сформулированной цели определять конкретные задачи для реализации поставленной цели. Владеть: – навыками выбора оптимального решения поставленной проблемы и достижения заявленной цели.
		ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и	ОПК-7.1 Знает базовые структуры данных; основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения. ОПК-7.2 Умеет применять известные методы программирования и возможности базового языка	Знать: – программные средства прикладного, системного и специального назначения, современные программные комплексы; – современные средства разработки и анализа программного обеспечения на языках высокого уровня. Уметь: – выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; – использовать языки программирования для решения

		способов организации программ	программирования для решения типовых профессиональных задач. ОПК-7.3 Владеет навыками разработки алгоритмов решения типовых профессиональных задач.	задач. Владеть: – навыками разработки программ на языке программирования высокого уровня; – навыками применения программных средств для решения конкретных задач; – навыками построения алгоритма и проведению его реализации в современных программных комплексах.
К.М.02.08	Основы управленческой деятельности	УК-2: Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает последовательность их реализации. УК-2.2. Формулирует проблему, на решение которой направлен проект, грамотно определяет цель проекта. УК-2.3. Проектирует решение конкретных задач проекта, выбирая оптимальный способ их решения.	Знать: – нормативно-правовую базу, регулирующую деятельность по управлению проектами. Уметь: – грамотно формулировать цель проекта; – исходя из сформулированной цели определять конкретные задачи для реализации поставленной цели. Владеть: – навыками выбора оптимального решения поставленной проблемы и достижения заявленной цели.
		УК-3: Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Разрабатывает командную стратегию для достижения поставленной цели. УК-3.2. Умеет организовывать и руководить работой команды. УК-3.3. Демонстрирует понимание результатов работы команды и личных действий в ней.	Знать: – основные принципы самообразования, профессионального и личностного развития. Уметь: – определять свои личные ресурсы и возможности для достижения поставленной цели. Владеть: – рационально распределять временные и/или иные ресурсы.
		УК-6: Способен определять и реализовывать приоритеты собственной деятельности и способы ее	УК-6.1. Применяет рефлексивные методы в процессе оценки разнообразных ресурсов, используемых для решения задач самоорганизации и саморазвития. УК-6.2. Определяет цели и	Знать: – рефлексивные методы в процессе оценки разнообразных ресурсов, используемых для решения задач самоорганизации и саморазвития. Уметь: – определять цели и приоритеты собственной деятельности и способы их достижения.

		совершенствования на основе самооценки и образования в течение всей жизни	приоритеты собственной деятельности и способы их достижения. УК-6.3. Планирует результаты собственной деятельности с учетом необходимых ресурсов.	Владеть: – навыками планирования результатов собственной деятельности с учетом необходимых ресурсов.
К.М.02.09	Управление IT-проектами	УК-2: Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает последовательность их реализации. УК-2.2. Формулирует проблему, на решение которой направлен проект, грамотно определяет цель проекта. УК-2.3. Проектирует решение конкретных задач проекта, выбирая оптимальный способ их решения.	Знать: – теоретические основы принятия решений в сфере управления IT-проектами. Уметь: – выявлять и анализировать различные способы решения задач в рамках цели IT-проекта и аргументирует их выбор. Владеть: – проектированием решения конкретной задачи IT-проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений.
		ПК-5: Способен управлять аналитическими работами и подразделениями	ПК-5.1. Обладает знаниями об управлении аналитическими ресурсами и компетенциями; об управлении процессами разработки и сопровождения требований к системам и управление качеством систем; об управлении инфраструктурой разработки и сопровождения требований к системе. ПК-5.2. Демонстрирует умения: разрабатывать технико-коммерческого предложения; разрабатывать методики выполнения аналитических работ; организовывать аналитические работы в ИТ-проекте; контролировать аналитические работы в ИТ-проекте. ПК-5.3. Имеет практический опыт (навыки): планирования аналитических работ в ИТ-проекте; составления отчетов об	Знать: – процессы жизненного цикла ПО, методы мониторинга и оценки качества процессов производственной деятельности, связанной с созданием и использованием информационных технологий. Уметь: – разрабатывать и реализовывать процессы жизненного цикла ПО; –реализовывать процессы управления качеством производственной деятельности, связанной с созданием и использованием информационных технологий; – осуществлять мониторинг и оценку качества процессов производственной деятельности. Владеть: использования методов и механизмов оценки и анализа функционирования средств ИТ; – навыки управления.

			аналитических работах в ИТ-проекте; оценки квалификации сотрудников в ИТ-проекте.	
К.М.03 Коммуникация и межкультурное взаимодействие				
К.М.03.01	История России	УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1 Обладает необходимыми знаниями о разнообразии культур и об основных принципах межкультурного взаимодействия. УК-5.2 Демонстрирует умение анализировать и использовать в профессиональной деятельности культурные и этические особенности среды. УК-5.3 Имеет навыки межкультурного взаимодействия при выполнении профессиональных задач. УК-5.4. Демонстрирует толерантное восприятие социальных и культурных различий, уважительное и бережное отношению к историческому наследию и культурным традициям. УК-5.5. Находит и использует необходимую для саморазвития и взаимодействия с другими людьми информацию о культурных особенностях и традициях различных социальных групп. УК-5.6. Проявляет в своём поведении уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России в контексте	Знать: – обладает базовыми знаниями об основных закономерностях социально-исторического развития общества и его культурном многообразии. Уметь: – демонстрирует умение понимать и толерантно воспринимать культурное многообразие общества в социально-историческом, этическом и философском контекстах. Владеть: – ориентируется в культурном разнообразии общества и соблюдает этические нормы поведения.

			мировой истории и культурных традиций мира. УК-5.7. Сознательно выбирает ценностные ориентиры и гражданскую позицию; аргументировано обсуждает и решает проблемы мировоззренческого, общественного и личностного характера	
		ОПК-17: Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	ОПК-17.1. Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира, выдающихся деятелей России. ОПК-17.2. Умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории России, опираясь на принципы историзма и научной объективности.	Знать: – основные этапы и закономерности исторического развития России. Уметь: – анализировать основные этапы и закономерности исторического развития , формулируя собственную точку зрения. Владеть: – приемами оценки исторических событий для формирования гражданской позиции.
К.М.03.02	Культура речи и деловое общение	УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах).	Знать: Для достижения УК-4.1 знать: основные понятия и теоретические положения изучаемой дисциплины; особенности и нормы употребления единиц различных уровней русского языка: фонетического (орфоэпия), грамматического (морфология и синтаксис, орфография и пунктуация), лексического (выбор слова, сочетаемость слов), словообразовательного (словообразование), стилистического (функциональные стили, стилистическая

		профессионального взаимодействия		окраска единиц, стилистическое единство текста); стиль делового общения, принципы деловой коммуникации в устной и письменной формах на государственном языке Российской Федерации. Уметь: Для достижения УК-4.1 уметь: создавать устные и письменные тексты в соответствии с нормами современного русского литературного языка, используя лингвистические словари и справочную литературу (ориентироваться в грамматических и стилистических пометах, различать общеязыковое и коннотативное значения слов и т.п.); строить деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации. Владеть: Для достижения УК-4.1 владеть: практическими навыками анализа устных и письменных текстов разных стилей и жанров; практическими навыками деловой коммуникации в устной и письменной формах на государственном языке Российской Федерации.
К.М.03.03	Иностранный язык	УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации на иностранном языке; профессиональной лексики на иностранном языке. УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном языке. УК-4.3. Владеет навыками академического и профессионального взаимодействия, в том числе на	Знать: Для достижения УК 4.1: лексику по изученным темам, грамматические конструкции соответствующего уровня, необходимые для осуществления академического и профессионального взаимодействия. Для достижения УК 4.2: структуру личного и делового письма, структуру устного сообщения(доклад, собеседование, публичное выступление и др.) Для достижения УК 4.3: современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия. Уметь: Для достижения УК 4.1: применять лексику по изученным темам в ситуациях академического и профессионального взаимодействия, использовать соответствующие грамматические конструкции в ситуациях академического и профессионального взаимодействия. Для достижения УК 4.2: писать личное и деловое письмо; делать устное сообщение; умеет применять коммуникативные технологии в разных моделях интернет-

			иностранном языке.	коммуникации. Для достижения УК 4.3: использовать соответствующие коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия. Владеть: Для достижения УК 4.1: правилами личной и профессиональной устной и письменной коммуникации. Для достижения УК 4.2: навыками выбора языковых средств в соответствии с задачами устной и письменной коммуникации. Для достижения УК 4.3: навыками организации работы (взаимодействия) проектной команды; навыками поиска информации, значимой для реализации проекта(для выполнения заданий).
К.М.03.04	Электроника и схемотехника	УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке(ах)	Знать: Для достижения индикатора УК-4.1: Знать правила профессиональной устной и письменной коммуникации для академического и профессионального взаимодействия Уметь: Для достижения индикатора УК-4.2: Уметь использовать современную измерительную литературу (в том числе на иностранном языке) при экспериментальном исследовании систем обработки информации Владеть: Для достижения индикатора УК-4.3: Владеть навыками использования современной научно-технической информацией (в том числе на иностранном языке) по электронике и схемотехнике
		ОПК-4: Способен анализировать	ОПК-4.1. Знает принципы работы элементов и	Знать: Для достижения индикатора ОПК-4.1: Знать основные

		физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	функциональных узлов электронной аппаратуры; методы анализа и синтеза электронных схем; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры. ОПК-4.2. Умеет работать с современной элементной базой электронной аппаратуры;использовать стандартные методы и средства проектирования цифровых узлов и устройств. ОПК-4.3. Владеет навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры; навыками чтения принципиальных схем, построения временных диаграмм работы узла, устройства по комплекту документации.	законы электричества и магнетизма; основы теории колебаний и волн; принципы работы элементов и функциональных узлов электронной аппаратуры; методы анализа и синтеза электронных схем; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры, архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры. Уметь: Для достижения индикатора ОПК-4.2: Умеет использовать математические модели физических явлений и процессов; решать типовые прикладные физические задачи; работать с современной элементной базой электронной аппаратуры; использовать стандартные методы и средства проектирования цифровых узлов и устройств; анализировать и синтезировать электронные схемы; определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств. Владеть: Для достижения индикатора ОПК-4.3: Владеть методами исследования физических явлений и процессов; навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры; навыками чтения принципиальных схем, построения временных диаграмм работы узла, устройства по комплекту документации; навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.
К.М.03.05	Администрирование Windows	УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах). УК-4.2. Демонстрирует умение применять современные	Знать: – основные термины и речевые обороты, употребляющиеся в сфере компьютерных технологий. Уметь: – составлять тексты и сообщения с описанием технологических и программных характеристик разрабатываемых продуктов. Владеть:

		академического и профессионального взаимодействия	коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке(ах).	– иметь навыки вербальной коммуникации на техническом иностранном языке.
		ОПК-12: Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	ОПК-12.1 Знает принципы построения современных операционных систем и особенности их применения; принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей; основные принципы конфигурирования и администрирования операционных систем. ОПК-12.2 Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; применять основные методы программирования в выбранной операционной среде.	Знать: – основные понятия защищенных операционных систем, баз данных и компьютерных сетей; – понятие защиты информации, системы защиты; – основные виды угроз безопасности информации и их классификацию; – основные понятия, основные алгоритмы хранения и обработки данных ОС; – основные стандарты и алгоритмы передачи данных; – основные актуальные модели атак; – аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; – средства аутентификации электронных данных и средства управления ключевой информацией; – требования к криптографическим системам защиты информации; – понятиями компьютерной безопасности в рамках администрирования и защиты публичных служб Windows. Уметь: – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами; – разрабатывать и конфигурировать программно-

			ОПК-12.3 Владеет навыками системного программирования; навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.	аппаратные средства защиты информации, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Владеть: – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети интернет; – основами конфигурирования и разработки программно-аппаратных средств защиты информации, системы управления базами данных; компьютерных сетей, системы антивирусной защиты, средств криптографической защиты информации в рамках администрирования и защиты публичных служб Windows.
К.М.03.06	Администрирование Linux и защита публичных служб	УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах). УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.3. Имеет навыки академического и профессионального	Знать: – основные термины и речевые обороты, употребляющиеся в сфере компьютерных технологий. Уметь: – составлять тексты и сообщения с описанием технологических и программных характеристик разрабатываемых продуктов. Владеть: – иметь навыки вербальной коммуникации на техническом иностранном языке.

			взаимодействия, в том числе на иностранном(ых) языке(ах).	
		ОПК-12: Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	ОПК-12.1 Знает принципы построения современных операционных систем и особенности их применения; принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей; основные принципы конфигурирования и администрирования операционных систем. ОПК-12.2 Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; применять основные методы программирования в выбранной операционной среде. ОПК-12.3 Владеет навыками системного программирования; навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.	Знать: – основные понятия операционных систем и их защиты; – основные понятия, основные алгоритмы хранения и обработки данных ОС; – основные стандарты и алгоритмы передачи данных; – основные актуальные модели атак. Уметь: – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети интернет.
К.М.03.07	Защита web-приложений	УК-4: Способен применять современные коммуникативные	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в	Знать: – основные термины и речевые обороты, употребляющиеся в сфере компьютерных технологий.

		технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	том числе на иностранном(ых) языке(ах). УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке(ах).	Уметь: – составлять тексты и сообщения с описанием технологических и программных характеристик разрабатываемых продуктов. Владеть: – иметь навыки вербальной коммуникации на техническом иностранном языке.
		ПК-4: Способен разрабатывать требования и рекомендации к системам защиты информации в web-приложениях	ПК-4.1. Обладает знаниями о формировании политик безопасности компьютерных систем; о разработке технических заданий на создание средств защиты информации; об определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; о требованиях к защите информации компьютерной системы; о разработке руководящих документов по защите информации. ПК-4.2. Демонстрирует умения: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия;	Знать: – основы политики безопасности компьютерных систем; – алгоритмы разработки технических заданий на создание средств защиты информации; – определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; – требования к защите информации компьютерной системы; – алгоритмы разработки руководящих документов по защите информации. Уметь: – 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; – формировать политики безопасности компьютерных систем и сетей.

			разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; формировать политики безопасности компьютерных систем и сетей. ПК-4.3. Имеет практический опыт (навыки): использования средств защиты информации; использования нормативные правовые акты в области защиты информации; разработки руководящих документов по защите информации.	Владеть: – навыками использования средств защиты информации; – навыками использования нормативных правовых актов в области защиты информации; – навыками разработки руководящих документов по защите информации.
К.М.03.08	Основы российской государственности	УК-5: Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1 Обладает необходимыми знаниями о разнообразии культур и об основных принципах межкультурного взаимодействия. УК-5.2 Демонстрирует умение анализировать и использовать в профессиональной деятельности культурные и этические особенности среды. УК-5.3 Имеет навыки межкультурного взаимодействия при выполнении профессиональных задач. УК-5.4. Демонстрирует толерантное восприятие социальных и культурных различий, уважительное и бережное отношению к историческому наследию и	Знать: Для достижения УК-5.4, УК-5.5, УК-5.6, УК-5.7 знать: о ключевых смыслах, этических и мировоззренческих доктринах, сложившихся внутри российской цивилизации и отражающих её многонациональный, многоконфессиональный и солидарный (общинный) характер; фундаментальные достижения, изобретения, открытия и свершения, связанные с развитием русской земли и российской цивилизации, представлять их в актуальной и значимой перспективе; о культурных особенностях и традициях различных социальных групп; о цивилизационном характере российской государственности, её основных особенностях, ценностных принципах и ориентирах; фундаментальные ценностные принципы российской цивилизации (такие как многообразие, суверенность, согласие, доверие и созидание); особенности современной политической организации

			культурным традициям. УК-5.5. Находит и использует необходимую для саморазвития и взаимодействия с другими людьми информацию о культурных особенностях и традициях различных социальных групп. УК-5.6. Проявляет в своём поведении уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России в контексте мировой истории и культурных традиций мира. УК-5.7. Сознательно выбирает ценностные ориентиры и гражданскую позицию; аргументировано обсуждает и решает проблемы мировоззренческого, общественного и личностного характера	российского общества, каузальную природу и специфику его актуальной трансформации, ценностное обеспечение традиционных институциональных решений и особую поливариантность взаимоотношений российского государства и общества в федеративном измерении; перспективные ценностные ориентиры российского цивилизационного развития (такие как стабильность, миссия, ответственность и справедливость); о наиболее вероятных внешних и внутренних вызовах, стоящих перед лицом российской цивилизации и её государственностью в настоящий момент, ключевых сценариях перспективного развития России;ть: Уметь: Для достижения УК-5.4, УК-5.5, УК-5.6, УК-5.7 уметь: толерантно воспринимать актуальные социальные и культурные различий, уважительно и бережно относиться к историческому наследию и культурным традициям; находить необходимую для саморазвития и взаимодействия с другими людьми информацию о культурных особенностях и традициях различных социальных групп; проявлять в своём поведении уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России в контексте мировой истории и культурных традиций мира; понимать ценностные ориентиры России и российского общества, а также вызовы и проблемы мировоззренческого, общественного и личностного характера; Владеть: Для достижения УК-5.4, УК-5.5, УК-5.6, УК-5.7 владеть навыками: толерантного поведения в отношение людей независимо от социальных и культурных различий; демонстрировать уважительное и бережное отношение к историческому наследию и культурным традициям; выстраивать взаимоотношения с людьми, понимая культурные особенности и традиции различных социальных групп; аргументированного обсуждения и решения проблем мировоззренческого, общественного и личностного

				характера; осознанного выбора ценностных ориентиров и гражданской позиции; развитого чувства гражданственности и патриотизма, самостоятельного критического мышления; решения вызовы и проблемы мировоззренческого, общественного и личностного характера.
К.М.04 Безопасность жизнедеятельности и здоровьесбережение				
К.М.04.01	Физическая культура и спорт	УК-7: Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Обладает знаниями здоровьесберегающих технологий для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности. УК-7.2. Демонстрирует умения поддержания должного уровня физической подготовленности и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности. УК-7.3- Имеет навыки поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.	Знать: – здоровьесберегающие технологии для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности Уметь: – поддерживать должный уровень физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: – навыками поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности
К.М.04.02	Безопасность жизнедеятельности	УК-8: Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности	УК-8.1. Идентифицирует опасности и оценивает факторы риска, опирается на принципы создания и поддержания безопасных условий жизнедеятельности для сохранения природной среды и обеспечения устойчивого	Знать: – опасности и оценивать факторы риска, опирается на принципы создания и поддержания безопасных условий жизнедеятельности, имеет представление об алгоритме оказания первой помощи, в том числе при возникновении чрезвычайных ситуаций. Уметь: – обеспечивать создание и поддержание безопасных

		для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	развития общества. УК-8.2. Обеспечивает создание и поддержание безопасных условий жизнедеятельности, оказания первой помощи в повседневной жизни и в профессиональной деятельности, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов. УК-8.3. Применяет способы и технологии создания и поддержания безопасных условий жизнедеятельности, в повседневной жизни и в профессиональной деятельности, алгоритм оказания первой помощи, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.	условий жизнедеятельности, оказания первой помощи, в том числе при возникновении чрезвычайных ситуаций. Владеть: – способами и технологиями создания и поддержания безопасных условий жизнедеятельности, алгоритм оказания первой помощи, в том числе при возникновении чрезвычайных ситуаций.
К.М.04.ДВ.01 Элективные дисциплины (модули) по физической культуре и спорту				
К.М.04.ДВ.01.01	Прикладная и оздоровительная физическая культура	УК-7: Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Обладает знаниями здоровьесберегающих технологий для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности. УК-7.2. Демонстрирует умения поддержания должного уровня физической подготовленности и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности. УК-7.3- Имеет навыки поддержания должного уровня	Знать: – здоровьесберегающие технологии для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности Уметь: – поддерживать должный уровень физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: – навыками поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности

			физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.деятельности.	
К.М.04.ДВ.01.02	Оздоровительная физическая культура	УК-7: Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Обладает знаниями здоровьесберегающих технологий для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности. УК-7.2. Демонстрирует умения поддержания должного уровня физической подготовленности и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности. УК-7.3- Имеет навыки поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.	Знать: – здоровьесберегающие технологии для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности Уметь: – поддерживать должный уровень физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: – навыками поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности
Б2 Практика				
Б2.О Обязательная часть				
Б2.О.01 Учебная практика				
Б2.О.01.01(У)	Учебно-лабораторный практикум	ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования	ОПК-7.1. Знает общие принципы построения, области и особенности применения языков программирования высокого и низкого уровня; язык программирования высокого и низкого уровня (объектно-ориентированное	Знать: - основные понятия информатики и языков программирования; - язык программирования С и основы языка программирования С++. Уметь: - применять программные средства для решения математических задач;

		для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	программирование); знает язык ассемблера персонального компьютера; базовые структуры данных; основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения. ОПК-7.2. Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого и низкого уровня алгоритмы решения типовых профессиональных задач; применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3. Владеет навыками разработки, документирования, тестирования и отладки программ; навыками разработки алгоритмов решения типовых профессиональных задач.	- использовать стандартные и сторонние библиотеки. Владеть: - навыками реализации базовых математических алгоритмов; - навыками работы в интегрированной среде разработки (IDE) MS Visual Studio.
		ПК-3: Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия	Знать: - базовые программные алгоритмы и структуры данных. Уметь: - применять базовые алгоритмы и структуры данных при решении прикладных задач. Владеть: - навыками реализации базовых алгоритмов.

			механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.	
Б2.О.02 Производственная практика				
Б2.О.02.01(Н)	Научно-исследовательская работа	ПК-1: Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; о порядке фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; о порядке проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о методах анализа систем обеспечения информационной безопасности	Знать: – основные принципы организации и использования всемирной сети Интернет. Уметь: – эффективно использовать программные средства для поиска в сети Интернет (браузеры, специализированные библиотечные программы). Владеть: – навыками эффективного поиска в всемирной сети Интернет; – навыками фильтрации получаемой информации.

			объектов информатизации на базе компьютерных систем в защищенном исполнении; о порядке подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; о методах проведения расследования компьютерных преступлений, правонарушений и инцидентов; о методах анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов. ПК-1.2. Демонстрирует умения: 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; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты	

			информации; прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов. ПК-1.3. Имеет практический опыт (навыки): составления экспертного заключения; установления участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация; определения механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям; определения причин и условий изменения свойств исследуемой информации; выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы; определения причин, целей и условий изменения свойств (состояния) программного обеспечения; индивидуального отождествления оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы.	
		ПК-2: Способен проводить мониторинг	ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных	Знать: – базовые технологии информационной безопасности и математический аппарат лежащий в их основе.

		защищенности компьютерных систем	атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет. ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки	Уметь: – грамотно использовать математический аппарат в решении прикладных задач. Владеть: – навыками научно-исследовательской работы, составления отчетной документации по ним.

			несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.	
		ПК-3: Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.	Знать: – стандарты в области безопасности компьютерных систем. Уметь: – производить анализ безопасности компьютерных систем на соответствие стандартам. Владеть: – навыками оценки безопасности компьютерных систем на соответствие стандартам.
		ПК-4: Способен разрабатывать требования и рекомендации к системам защиты информации в web-приложениях	ПК-4.1. Обладает знаниями о формировании политик безопасности компьютерных систем;о разработке технических заданий на создание средств защиты информации; об определении угроз безопасности	Знать: – математические модели безопасности компьютерных систем. Уметь: – проводить анализ математических моделей безопасности компьютерных систем. Владеть:

			информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; о требованиях к защите информации компьютерной системы; о разработке руководящих документов по защите информации. ПК-4.2. Демонстрирует умения: 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; формировать политики безопасности компьютерных систем и сетей. ПК-4.3. Имеет практический опыт (навыки): использования средств защиты информации; использования нормативные правовые акты в области защиты информации; разработки руководящих документов по защите информации.	– навыками разработки математических моделей безопасности компьютерных систем.
		ПК-5: Способен управлять аналитическими работами и	ПК-5.1. Обладает знаниями об управлении аналитическими ресурсами и компетенциями; об управлении процессами	Знать: – информацию об аналитических ресурсами и компетенциях; – информацию об управлении процессами разработки и

		подразделениями	разработки и сопровождения требований к системам и управление качеством систем; об управлении инфраструктурой разработки и сопровождения требований к системе. ПК-5.2. Демонстрирует умения: разрабатывать технико-коммерческого предложения; разрабатывать методики выполнения аналитических работ; организовывать аналитические работы в ИТ-проекте; контролировать аналитические работы в ИТ-проекте. ПК-5.3. Имеет практический опыт (навыки): планирования аналитических работ в ИТ-проекте; составления отчетов об аналитических работах в ИТ-проекте; оценки квалификации сотрудников в ИТ-проекте.	сопровождения требований к системам и управление качеством систем; – инфраструктуру разработки и сопровождения требований к системе. Уметь: – разрабатывать технико-коммерческие предложения; – разрабатывать методики выполнения аналитических работ; – организовывать аналитические работы в ИТ-проекте; – контролировать проведение аналитических работ в ИТ-проекте. Владеть: – навыками планирования аналитических работ в ИТ-проекте; – навыками составления отчетов об аналитических работах в ИТ-проекте; – навыками оценки квалификации сотрудников в ИТ-проекте.
Б2.О.02.02(П)	Технологическая практика	ПК-1: Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; о порядке фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; о порядке проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов; о способах обнаружения и нейтрализации последствий вторжений в компьютерные	Знать: – нормативные и правовые акты в сфере информационной безопасности. Уметь: – находить актуальную информацию в области компьютерной безопасности. Владеть: – методами поиска и анализа источников информации.

			системы; о методах анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; о порядке подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; о методах проведения расследования компьютерных преступлений, правонарушений и инцидентов; о методах анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов. ПК-1.2. Демонстрирует умения: 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; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой;	

			применять действующую законодательную базу в области обеспечения защиты информации; прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов. ПК-1.3. Имеет практический опыт (навыки): составления экспертного заключения; установления участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация; определения механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям; определения причин и условий изменения свойств исследуемой информации; выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы; определения причин, целей и условий изменения свойств (состояния) программного обеспечения; индивидуального отождествления оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы.	

		ПК-2: Способен проводить мониторинг защищенности компьютерных систем	ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет. ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых	Знать: – современные научные методы исследований в области информационной безопасности. Уметь: – применять теоретические знания для решения исследовательских задач. Владеть: – навыками проведения исследований в области защиты информации.

			сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.	
		ПК-3: Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.	Знать: – стандарты в области компьютерной безопасности. Уметь: – анализировать безопасность компьютерных систем. Владеть: – навыками оценки систем на соответствие стандартам безопасности.
		ПК-4: Способен разрабатывать требования и рекомендации к	ПК-4.1. Обладает знаниями о формировании политик безопасности компьютерных систем;о разработке технических	Знать: – математические модели безопасности компьютерных систем. Уметь:

		системам защиты информации в web-приложениях	заданий на создание средств защиты информации; об определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; о требованиях к защите информации компьютерной системы; о разработке руководящих документов по защите информации. ПК-4.2. Демонстрирует умения: 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; формировать политики безопасности компьютерных систем и сетей. ПК-4.3. Имеет практический опыт (навыки): использования средств защиты информации; использования нормативные правовые акты в области защиты информации; разработки руководящих документов по защите информации.	– производить анализ компьютерных систем. Владеть: – навыками разработки математических моделей безопасности.
		ПК-5: Способен	ПК-5.1. Обладает знаниями об	Знать:

		управлять аналитическими работами и подразделениями	управлении аналитическими ресурсами и компетенциями; об управлении процессами разработки и сопровождения требований к системам и управление качеством систем; об управлении инфраструктурой разработки и сопровождения требований к системе. ПК-5.2. Демонстрирует умения: разрабатывать технико-коммерческого предложения; разрабатывать методики выполнения аналитических работ; организовывать аналитические работы в ИТ-проекте; контролировать аналитические работы в ИТ-проекте. ПК-5.3. Имеет практический опыт (навыки): планирования аналитических работ в ИТ-проекте; составления отчетов об аналитических работах в ИТ-проекте; оценки квалификации сотрудников в ИТ-проекте.	– современные методы защиты информации с использованием программно-аппаратных средств защиты информации. Уметь: – проектировать комплексную систему защиты информации с использованием программно-аппаратных средств защиты информации. Владеть: – навыками разработки и конфигурации программно-аппаратных средств защиты информации.
Б2.О.02.03(Пд)	Преддипломная практика	ПК-1: Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; о порядке фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; о порядке проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов; о	Знать: – нормативные и правовые акты в сфере информационной безопасности. Уметь: – находить актуальную информацию в области компьютерной безопасности. Владеть: – методами поиска и анализа источников информации.

			способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о методах анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; о порядке подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; о методах проведения расследования компьютерных преступлений, правонарушений и инцидентов; о методах анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов. ПК-1.2. Демонстрирует умения: 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; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на	

			группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов. ПК-1.3. Имеет практический опыт (навыки): составления экспертного заключения; установления участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация; определения механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям; определения причин и условий изменения свойств исследуемой информации; выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы; определения причин, целей и условий изменения свойств (состояния) программного обеспечения; индивидуального отождествления оригинала программы (инсталляционной	

			версии) и ее копии на носителях данных компьютерной системы.	
		ПК-2: Способен проводить мониторинг защищенности компьютерных систем	ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет. ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с	Знать: – современные научные методы исследований в области информационной безопасности. Уметь: – применять теоретические знания для решения исследовательских задач. Владеть: – навыками проведения исследований в области защиты информации.

			использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.	
		ПК-3: Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.	Знать: – стандарты в области компьютерной безопасности. Уметь: – анализировать безопасность компьютерных систем. Владеть: – навыками оценки систем на соответствие стандартам безопасности.
		ПК-4: Способен	ПК-4.1. Обладает знаниями о	Знать:

		разрабатывать требования и рекомендации к системам защиты информации в web-приложениях	формировании политик безопасности компьютерных систем;о разработке технических заданий на создание средств защиты информации; об определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; о требованиях к защите информации компьютерной системы; о разработке руководящих документов по защите информации. ПК-4.2. Демонстрирует умения: 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; формировать политики безопасности компьютерных систем и сетей. ПК-4.3. Имеет практический опыт (навыки): использования средств защиты информации; использования нормативные правовые акты в области защиты информации; разработки руководящих документов по	– математические модели безопасности компьютерных систем. Уметь: – производить анализ компьютерных систем. Владеть: – навыками разработки математических моделей безопасности.

			защите информации.	
		ПК-5: Способен управлять аналитическими работами и подразделениями	ПК-5.1. Обладает знаниями об управлении аналитическими ресурсами и компетенциями; об управлении процессами разработки и сопровождения требований к системам и управление качеством систем; об управлении инфраструктурой разработки и сопровождения требований к системе. ПК-5.2. Демонстрирует умения: разрабатывать технико-коммерческого предложения; разрабатывать методики выполнения аналитических работ; организовывать аналитические работы в ИТ-проекте; контролировать аналитические работы в ИТ-проекте. ПК-5.3. Имеет практический опыт (навыки): планирования аналитических работ в ИТ-проекте; составления отчетов об аналитических работах в ИТ-проекте; оценки квалификации сотрудников в ИТ-проекте.	Знать: – информацию об аналитических ресурсами и компетенциях; – информацию об управлении процессами разработки и сопровождения требований к системам и управление качеством систем; – инфраструктуру разработки и сопровождения требований к системе. Уметь: – разрабатывать технико-коммерческие предложения; – разрабатывать методики выполнения аналитических работ; – организовывать аналитические работы в ИТ-проекте; – контролировать проведение аналитических работ в ИТ-проекте. Владеть: – навыками планирования аналитических работ в ИТ-проекте; – навыками составления отчетов об аналитических работах в ИТ-проекте; – навыками оценки квалификации сотрудников в ИТ-проекте.
Б2.В Часть, формируемая участниками образовательных отношений				
Б3 Государственная итоговая аттестация				
Б3.01(Г)	Подготовка к сдаче и сдача государственного экзамена	ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение	ОПК-1.1. Знает: понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики;	Знать: – основные термины по проблематике информационной безопасности; – цели, задачи, принципы и основные направления обеспечения информационной безопасности; – место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;

		для обеспечения объективных потребностей личности, общества и государства	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. ОПК-1.2. Умеет: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.	– содержание информационной войны, методы и средства ее ведения; – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Уметь: – пользоваться современной научно-технической информацией по исследуемым проблемам и задачам. Владеть: – навыками использования профессиональной терминологии в области информационной безопасности.
		ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере; логико-математические основы построения электронных цифровых устройств; состав, назначение аппаратных средств и программного обеспечения персонального компьютера, классификацию современных вычислительных систем, типовые структуры и принципы организации компьютерных сетей. ОПК-2.2. Умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет; составлять документы, используя прикладные программы офисного назначения;	Знать: – основные современные тенденции развития информатики и вычислительной техники; – организацию создания программных средств; – содержание различных этапов процесса разработки программных средств. Уметь: – работать с простейшими аппаратами, приборами и схемами, понимать принципы их действия; – использовать существующие пакеты прикладных программ для решения конкретных задач. Владеть: – приемами и методами решения конкретных задач из областей технологии, с учетом требований по обеспечению информационной безопасности; – навыками работы с программно-техническими средствами; – основными принципами организации и взаимодействия программных компонентов.

			средствами управления пользовательскими интерфейсами операционных систем. ОПК-2.3. Владеет средствами управления пользовательскими интерфейсами операционных систем; навыками системного программирования.	
		ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1.Знает основные задачи векторной алгебры и аналитической геометрии; возможности координатного метода для исследования различных геометрических объектов; основные виды уравнений простейших геометрических объектов; основные свойства важнейших алгебраических систем: групп, колец, полей; основы линейной алгебры и важнейшие свойства векторных пространств над произвольными полями; основные свойства колец многочленов над кольцами и полями; основные свойства отображений важнейших алгебраических систем; основные понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических	Знать: – основные математические методы. Уметь: – использовать математические методы и модели для решения задач профессиональной деятельности. Владеть: – математическими методами решения прикладных задач профессиональной деятельности.

			исчислений; основные способы задания булевых функций и функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов; свойства основных дискретных структур: линейных рекуррентных последовательностей, графов, конечных автоматов, комбинаторных структур; основные понятия и методы теории графов; основные понятия и методы теории конечных автоматов; основные понятия и методы комбинаторного анализа; основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных; основные методы дифференциального исчисления функций одной и нескольких действительных переменных; основные методы интегрального исчисления функций одной и нескольких действительных переменных; основные методы исследования числовых и функциональных рядов; основные задачи теории функций комплексного переменного; основные типы	

			обыкновенных дифференциальных уравнений и методы их решения; основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства; классические предельные теоремы теории вероятностей; основные понятия теории случайных процессов; постановку задач и основные понятия математической статистики; стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений; стандартные методы проверки статистических гипотез; основные понятия теории чисел; фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации; основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума; основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды – линейные, циклические, Хемминга); понятие пропускной способности канала связи,	

			прямую и обратную теоремы кодирования; основы теории нечетких множеств. ОПК-3.2. Умеет решать основные задачи линейной алгебры; решать основные задачи аналитической геометрии на плоскости и в пространстве; производить стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также оперировать с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; решать системы линейных уравнений над полями, приводить матрицы и квадратичные формы к каноническому виду; производить оценку качества полученных решений прикладных задач; производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы математической логики и теории алгоритмов к решению задач математической кибернетики; решать задачи периодичности и эквивалентности для линейных	

			рекуррентных последовательностей и конечных автоматов; применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; решать оптимизационные задачи на графах; применять стандартные методы дискретной математики для решения профессиональных задач; обосновывать основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных; обосновывать основные методы дифференциального исчисления функций одной и нескольких действительных переменных; обосновывать основные методы интегрального исчисления функций одной и нескольких действительных переменных; обосновывать основные методы исследования числовых и функциональных рядов; обосновывать классические положения и стандартные методы теории вероятностей и случайных процессов; обосновывать классические положения и стандартные методы математической статистики; разрабатывать и использовать вероятностные и статистические модели при решении типовых прикладных задач; решать основные типы задач теории чисел; вычислять	

			теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); решать типовые задачи кодирования и декодирования; работать с научно-технической литературой по тематике дисциплины; использовать методы на основе теории нечетких множеств для решения прикладных задач. ОПК-3.3. Владеет навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; методами решения стандартных алгебраических, матричных, подстановочных уравнений в алгебраических структурах; навыками решения типовых линейных уравнений над полем и кольцом вычетов; навыками решения стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований; навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению	

			переборных задач; навыками решения типовых комбинаторных и теоретико-графовых задач; навыками применения языка и средств дискретной математики при решении профессиональных задач; навыками использования справочных материалов по математическому анализу; основами построения математических моделей текстовой информации и моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач; навыками применения алгоритмов управления системами на основе правил нечеткого вывода.	
		ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Знает основные законы механики; основные законы термодинамики и молекулярной физики; основные законы электричества и магнетизма; основы теории колебаний и волн, оптики; основы квантовой физики и физики твёрдого тела; принципы работы элементов и функциональных узлов электронной аппаратуры; методы анализа и синтеза электронных схем; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; основные	Знать: – физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники; – базовые теоретические знания по физике; – смысл основных терминов и понятий физики. Уметь: – применять основные физические законы и модели для решения задач профессиональной деятельности; – пользоваться теоретическими знания и практическими навыками для решения задач профессиональной деятельности; – анализировать полученные экспериментальные данные. Владеть: – базовыми теоретическими знаниями и навыками лабораторных исследований в области физики; – навыком грамотного представления результатов

			телекоммуникационные протоколы; основные характеристики сигналов электросвязи, спектры и виды модуляции; принципы построения и функционирования систем и сетей передачи информации; способы передачи и распределения информации в телекоммуникационных системах и сетях; архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных мик-ропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры. ОПК-4.2. Умеет использовать математические модели физических явлений и процессов; решать типовые прикладные физические задачи; работать с современной элементной базой электронной аппаратуры; использовать стандартные методы и средства проектирования цифровых узлов и устройств; анализировать и синтезировать электронные схемы; определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и парамет-ры периферийных устройств. ОПК-4.3. Владеет методами	исследований и навыком оформления отчетов по лабораторным работам.

			исследования физических явлений и процессов; навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры; навыками чтения принципиальных схем, построения временных диаграмм работы узла, устройства по комплекту документации; пользоваться нормативными документами в области технической защиты информации; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.	
		ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1. Знает источники и классификацию угроз информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов	Знать: – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь: – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Владеть: – навыками работы с нормативными правовыми актами в области информационной безопасности; – навыками применения современной нормативной базы для построения системы организационных и программно-

			государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности. ОПК-5.2. Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах	технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.

			должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.	
		ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и	ОПК-6.1. Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны	Знать: – основные угрозы безопасности информации и модели нарушителя компьютерных систем; – систему нормативных правовых актов и стандартов по лицензированию в области защиты конфиденциальной информации. Уметь: – использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации;

		нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем. ОПК-6.2. разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.	– разрабатывать модели угроз и модели нарушителя компьютерных систем; – определить политику контроля доступа работников к информации ограниченного доступа; – формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; – применять отечественные и зарубежные стандарты в области компьютерной безопасности. Владеть: – навыками обеспечения использования правовых актов в своей профессиональной деятельности; – навыками защиты информации от утечки по техническим каналам.

		ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	ОПК-7.1. Знает общие принципы построения, области и особенности применения языков программирования высокого и низкого уровня; язык программирования высокого и низкого уровня (объектно-ориентированное программирование); знает язык ассемблера персонального компьютера; базовые структуры данных; основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения. ОПК-7.2. Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого и низкого уровня алгоритмы решения типовых профессиональных задач; применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3. Владеет навыками разработки, документирования, тестирования и отладки программ; навыками разработки	Знать: – специфику создания низкоуровневого кода под современные процессоры. – современные средства разработки и анализа программного обеспечения на языках высокого уровня; – программные средства прикладного, системного и специального назначения, современные программные комплексы; – архитектуру и программный интерфейс современных операционных систем. Уметь: – проектировать программное обеспечение с учётом низкоуровневой специфики архитектуры современных процессоров; – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; – выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; – создавать код любой сложности под современные процессоры; – создавать прикладное и системное программное обеспечение для современных операционных систем. Владеть: – навыками реализации программного обеспечения любой сложности с использованием высокоуровневых и низкоуровневых языков программирования.

			алгоритмов решения типовых профессиональных задач.	
		ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-8.1. Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; средства и методы хранения и передачи и анализа конфиденциальной информации; основные методы научных исследований при разработке моделей безопасности компьютерных систем. ОПК-8.2. Умеет разрабатывать модели обнаружения угроз и модели обнаружения нарушителя безопасности компьютерных систем; применять методы научных исследований при проведении разработок моделей безопасности компьютерных систем. ОПК-8.3. Владеет способами моделирования безопасности компьютерных систем.	Знать: – виды и состав угроз информационной безопасности; – принципы и общие методы обеспечения информационной безопасности; – источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; – каналы и методы несанкционированного доступа к конфиденциальной информации; – состав объектов защиты информации. Уметь: – определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию; – определять возможные каналы и методы несанкционированного доступа; – принимать решения при выборе средств защиты информации на основе анализа угроз и рисков; – организовывать системное обеспечение защиты информации. Владеть: – навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий; – навыками разработки основных политик безопасности.
		ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях	ОПК-9.1. Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; возможности технических средств перехвата информации;	Знать: – основные понятия операционных систем и их защиты; – основные понятия, основные алгоритмы хранения и обработки данных ОС; – основные стандарты и алгоритмы передачи данных; – основные понятия защищенных операционных систем, баз данных и компьютерных сетей; – основные актуальные модели атак; – понятие защиты информации, системы защиты; – аппаратно-программные средства защиты информации: – средства обеспечения конфиденциальности данных;

		и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	методы защиты и средства обеспечения безопасности в операционных системах, компьютерных сетях и системах управления базами данных; методы предотвращения и обнаружения вторжений в операционных системах, компьютерных сетях и системах управления базами данных; технические каналы утечки информации. ОПК-9.2. Умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации; осуществлять меры противодействия нарушениям безопасности в операционных системах, компьютерных сетях и системах управления базами данных с использованием различных программных и аппаратных средств защиты. ОПК-9.3. Владеет методами и средствами технической защиты информации.	– средства аутентификации электронных данных и средства управления ключевой информацией; – цели и концептуальные основы защиты информации; – основные виды угроз безопасности информации и их классификацию. Уметь: – осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации; – оценивать угрозы безопасности клиентским ОС осуществлять проверку защищенности клиентских ОС; – осуществлять проверку защищенности серверных ОС; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – навыками настройки политики безопасности и учетных записей ОС оценки степени защищенности клиентских ОС; – навыками оценки степени безопасности ОС; – навыками администрирования протокольных средств обеспечения безопасности ОС; – навыками администрирования прав пользователей и аудита доступа к ресурсам ОС; – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети

				интернет.
		ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. Знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; базовые понятия теории эллиптических кривых; типовые криптопротоколы, используемые в сетях связи; основные типы криптопротоколов и принципов их построения с использованием шифрсистем; основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты; основные типы криптографических методов защиты информации. ОПК-10.2. Умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях; исследовать и решать сравнения в кольцах вычетов; использовать достаточные условия простоты для построения больших простых чисел; оценивать теоретическую сложность применяемых алгоритмов;	Знать: – основные понятия и классификацию средств криптографической защиты информации; – различия между стеганографией и криптографией; – основные методы симметричного шифрования; – классификацию методов симметричного шифрования; – основные свойства симметричных криптосистем; – понятие хеш-функции; – основные понятия, основные алгоритмы электронной цифровой подписи; – основные стандарты на алгоритмы цифровой подписи; – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. Уметь: – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и

			разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; проводить анализ криптографической стойкости хеш-функции, в том числе с использованием автоматизированных средств. ОПК-10.3. Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел; подходами к разработке и анализу безопасности криптографических протоколов; навыками использования типовых криптографических алгоритмов; подходами к разработке и анализу безопасности криптографических хеш-функции.	распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – основными методами симметричного шифрования; алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет. – основными методами симметричного шифрования; алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.
		ОПК-11. . Способен разрабатывать политики	ОПК-11.1. Знает основные понятия и определения, используемые при описании	Знать: – типовые модели политик безопасности КС, политик управления доступом и информационными потоками.

		безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	моделей безопасности компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков. ОПК-11.2. Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками. ОПК-11.3. Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	Уметь: – самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности, управления доступом и информационными потоками, с учетом заданных требований. Владеть: – методами разработки моделей политик безопасности, управления доступом и информационными потоками.
		ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного	ОПК-12.1. Знает принципы построения современных операционных систем и особенности их применения; принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их	Знать: – общее устройство принципы работы современных операционных систем (ОС); – назначение и организацию основных служебных структур данных; – принципы работы механизмов защиты операционных систем семейств Windows и Linux. Уметь: – выполнять установку, настройку, обслуживание современных ОС.

		обеспечения	недокументированных возможностей; основные принципы конфигурирования и администрирования операционных систем. ОПК-12.2. Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; применять основные методы программирования в выбранной операционной среде. ОПК-12.3.1 Владеет навыками системного программирования; навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.	Владеть: – навыками настройки учетных записей ОС.
		ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ОПК-13.1. Знает средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки	Знать: – цели и концептуальные основы защиты информации; – основные виды угроз безопасности информации и их классификацию; – программно-аппаратные средства защиты информации: – средства обеспечения конфиденциальности данных; – средства аутентификации электронных данных и средства управления ключевой информацией; – требования к криптографическим системам защиты информации; – понятие и виды криптографических атак. Уметь: – оценивать угрозы безопасности клиентским ОС; – проектировать и использовать системы электронной цифровой подписи;

			по техническим каналам на объектах информатизации; основы физической защиты объектов информатизации. ОПК-13.2. Умеет формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем; пользоваться нормативными документами в области технической защиты информации; анализировать и оценивать угрозы информационной безопасности объекта. ОПК-13.3. Владеет методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей эффективности технической защиты информации.	– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем; – использовать алгоритмы генерации, хранения и распределения ключей; – осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации; – осуществлять проверку защищенности клиентских ОС; – осуществлять проверку защищенности серверных ОС. Владеть: – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети интернет.
		ОПК-14. Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации	ОПК-14.1. Знает характеристики и типы систем баз данных; основные языки запросов; физическую организацию баз данных и принципы (основы) их защиты; общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения	Знать: – характеристики и типы систем баз данных; – этапы проектирования баз данных; – физическую организацию баз данных; – основные модели структур данных; – способы организации файловых систем; – основные понятия о реляционной модели данных; – основные предложения языка запросов SQL; – области применения систем управления базами данных; – средства поддержания целостности в базах данных; – особенности управления данными в системах

			конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в СУБД; этапы проектирования системы защиты в СУБД. ОПК-14.2. Умеет проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных; настраивать и применять современные системы управления базами данных; пользоваться средствами защиты, предоставляемыми СУБД; создавать дополнительные средства защиты баз данных; проводить анализ и оценивание механизмов защиты баз данных. ОПК-14.3. Владеет методикой и навыками составления запросов для поиска информации в базах данных; методикой и навыками использования средств защиты, предоставляемых СУБД.	распределенной обработки; – порядок эксплуатации баз данных. Уметь: – разрабатывать программы на языках программирования четвертого поколения; – реализовывать на практике сложные структуры данных средствами реляционной СУБД; – использовать язык запросов SQL; – отображать предметную область на конкретную модель данных; – приводить в соответствие отношения при проектировании реляционной базы данных. Владеть: – навыками разработчика и администратора баз данных; – навыками поддержки и сопровождения баз данных; – навыками резервного копирования данных; – навыками обоснованного выбора инструментальных систем разработки баз данных; – навыками работы со средствами поддержания интерфейса с различными категориями пользователей СУБД; – навыками работы с системами управления базами данных на различных платформах.
		ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования	ОПК-15.1. Знает архитектуру основных типов современных компьютерных систем; принципы построения современных операционных систем и особенности их применения; основы организации и построения компьютерных сетей; эталонную модель взаимодействия	Знать: – задачи и цели администрирования сетевой инфраструктуры организации; – основы функционирования сетевых протоколов и служб; – функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печати, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов; – принципы построения системы безопасности сетевой операционной системы;

			открытых систем; функции, принципы действия и алгоритмы работы сетевого оборудования; основы организации и построения беспроводных компьютерных сетей. ОПК-15.2. Умеет реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования компьютерных сетей; реализовывать приложения для беспроводных сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования беспроводных компьютерных сетей. ОПК-15.3. Владеет навыками администрирования компьютерных сетей; навыками работы с сетевым оборудованием и сетевым программным обеспечением; навыками администрирования беспроводных компьютерных сетей; навыками работы с беспроводным сетевым оборудованием и сетевым программным обеспечением.	– задачи и цели администрирования беспроводной сетевой инфраструктуры; – основы функционирования беспроводных сетевых протоколов и служб; – принципы построения системы безопасности беспроводной сетевой инфраструктуры. Уметь: – проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации; – производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы; – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности; – проектировать беспроводную сетевую инфраструктуру в соответствии с потребностями построения информационной системы; – производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы; – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности. Владеть: – технологиями и навыками построения и администрирования службы каталогов информационной системы организации; – инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования; – методами и средствами аудита и мониторинга сетевых устройств и служб.; – технологиями и навыками построения и администрирования беспроводной сетевой инфраструктуры; – методами и средствами аудита и мониторинга беспроводных сетевых устройств и служб.
		ОПК-16. Способен	ОПК-16.1. Знает средства и	Знать:

		проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений; общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в СУБД; этапы проектирования системы защиты в СУБД. ОПК-16.2. Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с	– угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем; – типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем; – условия их осуществимости, возможные последствия, способы предотвращения; – угрозы и методы нарушения информационной безопасности БД; – типовые модели атак, направленных на преодоление защиты БД; – условия их осуществимости, возможные последствия, способы предотвращения. Уметь: – устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем; – устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем, БД. Владеть: – навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в сетях; – навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в БД.

			использованием различных программных и аппаратных средств защиты; пользоваться средствами защиты, предоставляемыми СУБД; создавать дополнительные средства защиты баз данных; проводить анализ и оценивание механизмов защиты баз данных. ОПК-16.3. Владеет навыками настройки межсетевых экранов; методиками анализа сетевого трафика; методикой и навыками использования средств защиты, предоставляемых СУБД.	
		ОПК-17. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-17.1. Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира, выдающихся деятелей России. ОПК-17.2. Умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории России, опираясь на принципы историзма и научной объективности.	Знать: – основные этапы и закономерности исторического развития России. Уметь: – анализировать основные этапы и закономерности исторического развития , формулируя собственную точку зрения. Владеть: – приемами оценки исторических событий для формирования гражданской позиции.
		ОПК-1.1. Способен проводить анализ	ОПК 1.1.1. Знает принципы построения защищенных	Знать: – российские и зарубежные стандарты в области

		защищенности и осуществлять поиск уязвимостей компьютерной системы	компьютерных систем и сетей; требования основных стандартов по оценке защищенности компьютерных систем и сетей; основные типы уязвимостей программного обеспечения; виды атак и механизмы их реализации в компьютерных системах; принципы построения защищенных компьютерных систем и сетей. ОПК 1.1.2. Умеет определять уровень защищенности и доверия программно-аппаратных средств защиты информации; классифицировать информационные системы по требованиям защиты информации; определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе; выполнять анализ компьютерной системы с целью определения уровня защищенности и доверия; проводить теоретические исследования уровней защищенности и доверия компьютерных систем и сетей; применять средства и методы анализа программных реализаций для поиска уязвимостей.	информационной безопасности; – современные критерии и стандарты для анализа безопасности компьютерных систем; – особенности программирования шеллкодов; – методы исследования программного обеспечения без исходных кодов. Уметь: – оценивать соответствие проектной и эксплуатационной документации информационной системы на соответствие стандарту в области информационной безопасности; – применять современные критерии и стандарты для анализа безопасности компьютерных систем; – создавать шеллкоды для современных операционных системы под разные аппаратные платформы; – исследовать программное обеспечение без исходных кодов. Владеть: – практическими навыками оценки защищенности на соответствие стандартам информационной безопасности ЦБ РФ в области информационных систем, функционирующих в финансовой сфере; – практическими навыками работы с современными критериями и стандартами для анализа безопасности компьютерных систем; – навыками создания шеллкодов с учетом специфики различных сценариев использования; – навыками использования современных средств исследования программного обеспечения без исходных кодов.
		ОПК-1.2. Способен оценивать корректность программных	ОПК 1.2.1. Знает основные средства и методы защиты программного обеспечения от анализа и нарушения	Знать: – базовые методы функционирования вредоносного программного обеспечения; – методы защиты программного обеспечения от

		реализаций алгоритмов защиты информации	целостности; основные программные методы защиты данных от несанкционированного доступа; теоретические основы устранения избыточности данных; основные алгоритмы кодирования данных и сжатия текстовой, графической, аудио- и видеоинформации; основные средства и методы защиты программного обеспечения от анализа и нарушения целостности. ОПК 1.2.2 Умеет проводить анализ программных средств, применяемых для контроля и защиты информации; проводить анализ программ и алгоритмов на предмет соответствия требованиям защиты информации; проводить анализ программ и алгоритмов сжатия данных на предмет соответствия требованиям защиты информации.	исследования, копирования, модификации; – форматы графических данных; – дискретное преобразование Фурье; – вейвлетные преобразования; – кодирование источников информации; – словарные методы сжатия; – блочно-сортирующим сжатие. Уметь: – реализовывать базовые функциональные компоненты вредоносного программного обеспечения; – реализовывать методы защиты программного обеспечения от исследования с учетом специфики операционных систем, аппаратной платформы, используемой архитектуры; – разрабатывать и реализовывать алгоритмы кодирования и сжатия различных видов информации. Владеть: – навыками исследования вредоносного программного обеспечения с использованием современных инструментов анализа и собственных утилит; – навыками реализации методов защиты программного обеспечения от исследования и обхода этих методов; – методами оценки эффективности алгоритмов кодирования и сжатия различных видов информации.
		ОПК-1.3. Способен проводить тестирование и использовать средства верификации механизмов защиты информации	ОПК 1.3.1 Знает основные способы и средства верификации программ; основные способы тестирования средств защиты информации с использованием средств верификации программ; основные способы и средства верификации программ. ОПК 1.3.2 Умеет применять основные методы верификации программ и алгоритмов на предмет соответствия	Знать: – основы построения и реализации биометрических систем аутентификации, – основы тестирования и оценки надежности разработанных биометрических систем аутентификации. Уметь: – самостоятельно строить и анализировать алгоритмы, которые используются для построения биометрических систем аутентификации. Владеть: – навыками построения алгоритмов для биометрических систем аутентификации и проведения тестирования разработанных алгоритмов.

			требованиям защиты информации.	
		ПК-1. Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; о порядке фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; о порядке проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о методах анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; о порядке подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; о методах проведения расследования компьютерных преступлений, правонарушений и инцидентов; о методах анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов. ПК-1.2. Демонстрирует умения:	Знать: – основные принципы организации и использования всемирной сети Интернет; – нормативные и правовые акты в сфере информационной безопасности. Уметь: – эффективно использовать программные средства для поиска в сети Интернет (браузеры, специализированные библиотечные программы); – находить актуальную информацию в области компьютерной безопасности. Владеть: – навыками эффективного поиска в всемирной сети Интернет; – навыками фильтрации получаемой информации; – методами анализа источников информации.

			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; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов. ПК-1.3. Имеет практический опыт (навыки): составления экспертного заключения; установления участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация; определения механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям; определения	

			причин и условий изменения свойств исследуемой информации; выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы; определения причин, целей и условий изменения свойств (состояния) программного обеспечения; индивидуального отождествления оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы.	
		ПК-2. Способен проводить мониторинг защищенности компьютерных систем и сетей	ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2. Демонстрирует умения: формализовывать задачу	Знать: – общие положения интернета вещей; – стандарты и протоколы передачи данных в IoT; – практическую реализацию IoT; – принципы построения систем обнаружения компьютерных атак; – актуальные методы обработки данных мониторинга безопасности компьютерных систем и сетей; – нормативные правовые акты в области защиты информации; – архитектуру MPLS VPN; – базовые концепции MPLS; – модели Overlay VPN и Peer-to-Peer VPN; – назначение и распределение меток в сети MPLS; – основные концепции проектирования компьютерных сетей; – основы построения вычислительных сетей предприятия; – основы функционирования сетевых протоколов и служб; – понятие инфраструктуры корпоративной сети; – понятия и технологии корпоративных сетей, сетей LAN, сетей WAN; – принципы адресации и коммутации в корпоративной сети;

			управления безопасностью компьютерных систем; применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет. ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.	– принципы использования IP-адресации в проекте компьютерной сети; – принципы построения системы безопасности сетевой операционной системы; – терминологию и архитектуру MPLS; – функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печа-ти, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов; – эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы. Уметь: – решать задачу управления безопасностью компьютерных систем; – применять инструментальные средства проведения мониторинга защищенности компьютерных систем; – применять методы анализа защищенности компьютерных систем и сетей; – структурировать аналитическую информацию для включения в отчет; – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности; – внедрять списки доступа, позволяющие разрешать или отклонять трафик определенного типа; – настраивать протоколы маршрутизации устройств Cisco; – настраивать фильтрацию трафика с использованием списков контроля доступа; – описывать существующую компьютерную сеть, определять требования (влияние используемых приложений, требования пользователей, технические параметры и др.); – проводить испытания на прототипе сети WAN и устранять неполадки в корпоративных сетях; – проектировать простую компьютерную сеть с использованием технологий Cisco (разрабатывать схему IP-адресации, соответствующую требованиям локальной компьютерной сети; составлять список оборудования, соответствующего требованиям проекта локальной компьютерной сети; получать и обновлять программное

				обеспечение Cisco IOS для устройств Cisco); – получать и обновлять программное обеспечение Cisco IOS для устройств Cisco); – проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации; – производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы; – работать с протоколом VTP; – работать с протоколом связующего дерева STP; – разрабатывать и конфигурировать MPLS VPN; – разрабатывать технические и коммерческие предложения по созданию и модернизации компьютерной сети для комплекса зданий; – создавать каналы в корпоративной сети WAN; – создавать локальную сеть в соответствии с утвержденным проектом: настраивать коммутатор с поддержкой технологии VLAN и соединений между коммутаторами. Владеть: – навыками практической реализации IoT; – навыками анализа защищенности компьютерных систем с использованием сканеров безопасности; – навыками анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; – навыками составления отчетов по результатам проверок; – инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования; – методами и средствами аудита и мониторинга сетевых устройств и служб; – методикой анализа сетевого трафика; – навыками анализа требований заказчика и проектирования компьютерной сети; – навыками анализа, проектирования и настройки схем потоков трафика в компьютерной сети; – навыками мониторинга работы сети, обследования и

				модернизации сетевого оборудования; – навыками настройки коммутации в корпоративной сети; – навыками настройки адресации в сети на базе технологий VLSM, NAT и PAT; – навыками настройки механизмов фильтрации трафика на базе списков контроля доступа (ACL); – навыками настройки протоколов маршрутизации на базе протоколов RIPv2, EIGRP, OSPF; – навыками определения влияния приложений на проект сети; – навыками оценки качества и соответствия требованиям проекта сети; – навыками работы с виртуальными сетями VLAN; – навыками создания и настройки каналов корпоративной сети на базе технологий PPP, PAP, CHAP и Frame Relay; – навыками устранения проблем коммутации, связи, маршрутизации и конфигурации WAN; – навыками фильтрации, контроля и обеспечения безопасности сетевого трафика; – технологиями и навыками построения и администрирования службы каталогов информационной системы организации.
		ПК-3. Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности	Знать: - базовые программные алгоритмы и структуры данных. – роль эллиптических кривых в современных асимметричных шифрах; – формальные требования, предъявляемые к криптографическим эллиптическим кривым; – методы проникновения в компьютерные системы, используемые современным вредоносным программным обеспечением; – методы функционирования современного вредоносного программного обеспечения. Уметь: - применять базовые алгоритмы и структуры данных при решении прикладных задач. – анализировать криптографические эллиптические кривые на предмет их защищённости;

			программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.	– конструировать эллиптические кривые, обладающие заданными свойствами; – реализовывать современные атаки на компьютерные системы; – исследовать вредоносное программное обеспечение. Владеть: - навыками реализации базовых алгоритмов. – навыками разработки и конфигурирования программно-аппаратных средств криптографической защиты информации, основанных на криптографических эллиптических кривых; – инструментами проведения современных атак на компьютерные системы; – навыками использования инструментальных средств исследования вредоносного программного обеспечения.
		ПК-4. Способен разрабатывать требования и рекомендации к системам защиты информации в web-приложениях	ПК-4.1. Обладает знаниями о формировании политик безопасности компьютерных систем; о разработке технических заданий на создание средств защиты информации; об определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; о требованиях к защите информации компьютерной системы; о разработке руководящих документов по защите информации. ПК-4.2. Демонстрирует умения: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты	Знать: – математические модели безопасности компьютерных систем. Уметь: – проводить анализ математических моделей безопасности компьютерных систем. Владеть: – навыками разработки математических моделей безопасности компьютерных систем.

			компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; формировать политики безопасности компьютерных систем и сетей. ПК-4.3. Имеет практический опыт (навыки): использования средств защиты информации; использования нормативные правовые акты в области защиты информации; разработки руководящих документов по защите информации.	
		ПК-5. Способен управлять аналитическими работами и подразделениями	ПК-5.1. Обладает знаниями об управлении аналитическими ресурсами и компетенциями; об управлении процессами разработки и сопровождения требований к системам и управление качеством систем; об управлении инфраструктурой разработки и сопровождения требований к системе. ПК-5.2. Демонстрирует умения: разрабатывать технико-коммерческого предложения; разрабатывать методики выполнения аналитических работ; организовывать аналитические работы в ИТ-проекте; контролировать аналитические работы в ИТ-проекте. ПК-5.3. Имеет практический	Знать: – информацию об аналитических ресурсами и компетенциях; – информацию об управлении процессами разработки и сопровождения требований к системам и управление качеством систем; – инфраструктуру разработки и сопровождения требований к системе. Уметь: – разрабатывать технико-коммерческие предложения; – разрабатывать методики выполнения аналитических работ; – организовывать аналитические работы в ИТ-проекте; – контролировать проведение аналитических работ в ИТ-проекте. Владеть: – навыками планирования аналитических работ в ИТ-проекте; – навыками составления отчетов об аналитических работах в ИТ-проекте; – навыками оценки квалификации сотрудников в ИТ-

			опыт (навыки): планирования аналитических работ в ИТ-проекте; составления отчетов об аналитических работах в ИТ-проекте; оценки квалификации сотрудников в ИТ-проекте.	проекте.
Б3.02(Д)	Подготовка к процедуре защиты и защита выпускной квалификационной работы	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Критически анализирует проблемную ситуацию с целью выработки стратегии действий, аргументировано формулирует собственные суждения и оценки УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения проблемной ситуации	Знать: – основные положения теории систем, функциональных систем и генетических, саморазвивающихся систем. Уметь: – осуществлять поиск, критический анализ проблемных ситуаций на основе системного подхода, – вырабатывать стратегию действий. Владеть: – способами поиска и критического анализа проблемных ситуаций на основе системного подхода, – способами разработки стратегии действий.
		УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает последовательность их реализации. УК-2.2. Формулирует проблему, на решение которой направлен проект, грамотно определяет цель проекта. УК-2.3. Проектирует решение конкретных задач проекта, выбирая оптимальный способ их решения.	Знать: – нормативно-правовую базу, регулирующую деятельность по управлению проектами. Уметь: – грамотно формулировать цель проекта; – исходя из сформулированной цели определять конкретные задачи для реализации поставленной цели. Владеть: – навыками выбора оптимального решения поставленной проблемы и достижения заявленной цели.
		УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Разрабатывает командную стратегию для достижения поставленной цели. УК-3.2. Умеет организовывать и руководить работой команды. УК-3.3. Демонстрирует понимание результатов работы команды и личных действий в ней.	Знать: – основные принципы самообразования, профессионального и личностного развития. Уметь: – определять свои личные ресурсы и возможности для достижения поставленной цели. Владеть: – рационально распределять временные и/или иные ресурсы.

		УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке(ах)	Знать: – основные понятия и теоретические положения изучаемой дисциплины; – стиль делового общения, принципы деловой коммуникации в устной и письменной формах на государственном языке Российской Федерации; – правила профессиональной устной и письменной коммуникации для академического и профессионального взаимодействия; – современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия. Уметь: – создавать устные и письменные тексты в соответствии с нормами современного русского литературного языка, используя лингвистические словари и справочную литературу; – строить деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации; – использовать современную измерительную литературу (в том числе на иностранном языке) при экспериментальном исследовании систем обработки информации. Владеть: – практическими навыками деловой коммуникации в устной и письменной формах на государственном языке Российской Федерации; – навыками организации работы (взаимодействия) проектной команды; навыками поиска информации, значимой для реализации проекта(для выполнения заданий). – навыками использования современной научно-технической информацией (в том числе на иностранном языке).
		УК-5. Способен анализировать и учитывать разнообразие культур	УК-5.1 Обладает необходимыми знаниями о разнообразии культур и об основных принципах межкультурного	Знать: – процессы жизненного цикла ПО, методы мониторинга и оценки качества процессов производственной деятельности, связанной с созданием и использованием информационных

		в процессе межкультурного взаимодействия	взаимодействия УК-5.2 Демонстрирует умение анализировать и использовать в профессиональной деятельности культурные и этические особенности среды. УК-5.3 Имеет навыки межкультурного взаимодействия при выполнении профессиональных задач	технологий. Уметь: – разрабатывать и реализовывать процессы жизненного цикла ПО; –реализовывать процессы управления качеством производственной деятельности, связанной с созданием и использованием информационных технологий; – осуществлять мониторинг и оценку качества процессов производственной деятельности. Владеть: использования методов и механизмов оценки и анализа функционирования средств ИТ; – навыки управления.
		УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК-6.1. Применяет рефлексивные методы в процессе оценки разнообразных ресурсов, используемых для решения задач самоорганизации и саморазвития. УК-6.2. Определяет цели и приоритеты собственной деятельности и способы их достижения. УК-6.3. Планирует результаты собственной деятельности с учетом необходимых ресурсов.	Знать: – рефлексивные методы в процессе оценки разнообразных ресурсов, используемых для решения задач самоорганизации и саморазвития. Уметь: – определять цели и приоритеты собственной деятельности и способы их достижения. Владеть: – навыками планирования результатов собственной деятельности с учетом необходимых ресурсов.
		УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1.Обладает знаниями здоровьесберегающих технологий для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности. УК-7.2. Демонстрирует умения поддержания должного уровня физической подготовленности и функциональной	Знать: – здоровьесберегающие технологии для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности Уметь: – поддерживать должный уровень физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: – навыками поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности

			подготовленности для обеспечения полноценной социальной и профессиональной деятельности. УК-7.3. Имеет навыки поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.	
		УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1. Идентифицирует опасности и оценивает факторы риска, опирается на принципы создания и поддержания безопасных условий жизнедеятельности для сохранения природной среды и обеспечения устойчивого развития общества. УК-8.2. Обеспечивает создание и поддержание безопасных условий жизнедеятельности, оказания первой помощи в повседневной жизни и в профессиональной деятельности, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов. УК-8.3. Применяет способы и технологии создания и поддержания безопасных условий жизнедеятельности, в повседневной жизни и в профессиональной деятельности, алгоритм оказания первой помощи, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.	Знать: – опасности и оценивать факторы риска, опирается на принципы создания и поддержания безопасных условий жизнедеятельности, имеет представление об алгоритме оказания первой помощи, в том числе при возникновении чрезвычайных ситуаций. Уметь: – обеспечивать создание и поддержание безопасных условий жизнедеятельности, оказания первой помощи, в том числе при возникновении чрезвычайных ситуаций. Владеть: – способами и технологиями создания и поддержания безопасных условий жизнедеятельности, алгоритм оказания первой помощи, в том числе при возникновении чрезвычайных ситуаций.
		УК-9. Способен	УК-9.1. Знает понятие	Знать:

		использовать базовые дефектологические знания в социальной и профессиональной сферах.	инклюзивной компетентности, ее компоненты и структуру, особенности применения базовых дефектологических знаний в социальной и профессиональной сферах. УК-9.2. Умеет планировать и осуществлять профессиональную деятельность с лицами с ограниченными возможностями здоровья. УК-9.3. Владеет навыками взаимодействия в социальной и профессиональной сферах с лицами с ограниченными возможностями здоровья.	– основные экономические категории и законы, принципы и методы экономического анализа. Уметь: – интерпретировать содержание социально-экономических процессов с точки зрения личных, коллективных и общественных интересов. Владеть: – способностью использовать экономические знания для принятия обоснованных экономических решений в различных областях жизнедеятельности.
		УК-10: Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1. Имеет представление о содержании понятия «коррупционное поведение», основных формах его проявления и последствиях. УК-10.2. Разграничивает коррупционные и схожие некоррупционные явления в различных сферах жизни общества. УК-10.3. Демонстрирует нетерпимое отношение к коррупционному поведению.	Знать: – понятие коррупции, коррупционного поведения; –положения антикоррупционного законодательства. Уметь: – применять нормы антикоррупционного законодательства. Владеть: – навыками применения норм антикоррупционного законодательства.
		ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных	ОПК-1.1. Знает: понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; основные средства и способы обеспечения информационной	Знать: – основные термины по проблематике информационной безопасности; – цели, задачи, принципы и основные направления обеспечения информационной безопасности; – место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; – содержание информационной войны, методы и средства ее ведения;

		потребностей личности, общества и государства	безопасности, принципы построения систем защиты информации. ОПК-1.2. Умеет: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.	– источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Уметь: – пользоваться современной научно-технической информацией по исследуемым проблемам и задачам. Владеть: – навыками использования профессиональной терминологии в области информационной безопасности.
		ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере; логико-математические основы построения электронных цифровых устройств; состав, назначение аппаратных средств и программного обеспечения персонального компьютера, классификацию современных вычислительных систем, типовые структуры и принципы организации компьютерных сетей. ОПК-2.2. Умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет; составлять документы, используя прикладные программы офисного назначения; средствами управления пользовательскими	Знать: – основные современные тенденции развития информатики и вычислительной техники; – организацию создания программных средств; – содержание различных этапов процесса разработки программных средств. Уметь: – работать с простейшими аппаратами, приборами и схемами, понимать принципы их действия; – использовать существующие пакеты прикладных программ для решения конкретных задач. Владеть: – приемами и методами решения конкретных задач из областей технологии, с учетом требований по обеспечению информационной безопасности; – навыками работы с программно-техническими средствами; – основными принципами организации и взаимодействия программных компонентов.

			интерфейсами операционных систем. ОПК-2.3. Владеет средствами управления пользовательскими интерфейсами операционных систем; навыками системного программирования.	
		ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1.Знает основные задачи векторной алгебры и аналитической геометрии; возможности координатного метода для исследования различных геометрических объектов; основные виды уравнений простейших геометрических объектов; основные свойства важнейших алгебраических систем: групп, колец, полей; основы линейной алгебры и важнейшие свойства векторных пространств над произвольными полями; основные свойства колец многочленов над кольцами и полями; основные свойства отображений важнейших алгебраических систем; основные понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности; язык и средства современной математической логики и теории логических исчислений; основные способы задания булевых функций и	Знать: – основные математические методы. Уметь: – использовать математические методы и модели для решения задач профессиональной деятельности. Владеть: – математическими методами решения прикладных задач профессиональной деятельности.

			функций многозначной логики формулами и их свойства; различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов; свойства основных дискретных структур: линейных рекуррентных последовательностей, графов, конечных автоматов, комбинаторных структур; основные понятия и методы теории графов; основные понятия и методы теории конечных автоматов; основные понятия и методы комбинаторного анализа; основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных; основные методы дифференциального исчисления функций одной и нескольких действительных переменных; основные методы интегрального исчисления функций одной и нескольких действительных переменных; основные методы исследования числовых и функциональных рядов; основные задачи теории функций комплексного переменного; основные типы обыкновенных дифференциальных уравнений и	

			методы их решения; основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства; классические предельные теоремы теории вероятностей; основные понятия теории случайных процессов; постановку задач и основные понятия математической статистики; стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений; стандартные методы проверки статистических гипотез; основные понятия теории чисел; фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации; основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума; основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды – линейные, циклические, Хемминга); понятие пропускной способности канала связи, прямую и обратную теоремы кодирования; основы теории	

			нечетких множеств. ОПК-3.2. Умеет решать основные задачи линейной алгебры; решать основные задачи аналитической геометрии на плоскости и в пространстве; производить стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также оперировать с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; решать системы линейных уравнений над полями, приводить матрицы и квадратичные формы к каноническому виду; производить оценку качества полученных решений прикладных задач; производить основные логические операции в исчислении высказываний и исчислении предикатов; находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; применять методы математической логики и теории алгоритмов к решению задач математической кибернетики; решать задачи периодичности и эквивалентности для линейных рекуррентных последовательностей и	

			конечных автоматов; применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; решать оптимизационные задачи на графах; применять стандартные методы дискретной математики для решения профессиональных задач; обосновывать основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных; обосновывать основные методы дифференциального исчисления функций одной и нескольких действительных переменных; обосновывать основные методы интегрального исчисления функций одной и нескольких действительных переменных; обосновывать основные методы исследования числовых и функциональных рядов; обосновывать классические положения и стандартные методы теории вероятностей и случайных процессов; обосновывать классические положения и стандартные методы математической статистики; разрабатывать и использовать вероятностные и статистические модели при решении типовых прикладных задач; решать основные типы задач теории чисел; вычислять теоретико-информационные характеристики источников	

			сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); решать типовые задачи кодирования и декодирования; работать с научно-технической литературой по тематике дисциплины; использовать методы на основе теории нечетких множеств для решения прикладных задач. ОПК-3.3. Владеет навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; методами решения стандартных алгебраических, матричных, подстановочных уравнений в алгебраических структурах; навыками решения типовых линейных уравнений над полем и кольцом вычетов; навыками решения стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований; навыками использования языка современной символической логики; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач; навыками решения типовых	

			комбинаторных и теоретико-графовых задач; навыками применения языка и средств дискретной математики при решении профессиональных задач; навыками использования справочных материалов по математическому анализу; основами построения математических моделей текстовой информации и моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач; навыками применения алгоритмов управления системами на основе правил нечеткого вывода.	
		ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Знает основные законы механики; основные законы термодинамики и молекулярной физики; основные законы электричества и магнетизма; основы теории колебаний и волн, оптики; основы квантовой физики и физики твёрдого тела; принципы работы элементов и функциональных узлов электронной аппаратуры; методы анализа и синтеза электронных схем; типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; основные телекоммуникационные протоколы; основные	Знать: – физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники; – базовые теоретические знания по физике; – смысл основных терминов и понятий физики. Уметь: – применять основные физические законы и модели для решения задач профессиональной деятельности; – пользоваться теоретическими знания и практическими навыками для решения задач профессиональной деятельности; – анализировать полученные экспериментальные данные. Владеть: – базовыми теоретическими знаниями и навыками лабораторных исследований в области физики; – навыком грамотного представления результатов исследований и навыком оформления отчетов по лабораторным работам.

			характеристики сигналов электросвязи, спектры и виды модуляции; принципы построения и функционирования систем и сетей передачи информации; способы передачи и распределения информации в телекоммуникационных системах и сетях; архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных мик-ропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры. ОПК-4.2. Умеет использовать математические модели физических явлений и процессов; решать типовые прикладные физические задачи; работать с современной элементной базой электронной аппаратуры; использовать стандартные методы и средства проектирования цифровых узлов и устройств; анализировать и синтезировать электронные схемы; определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и парамет-ры периферийных устройств. ОПК-4.3. Владеет методами исследования физических явлений и процессов; навыками	

			использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры; навыками чтения принципиальных схем, построения временных диаграмм работы узла, устройства по комплекту документации; пользоваться нормативными документами в области технической защиты информации; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.	
		ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1. Знает источники и классификацию угроз информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;	Знать: – источники и классификацию угроз информационной безопасности; – основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь: – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Владеть: – навыками работы с нормативными правовыми актами в области информационной безопасности; – навыками применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.

			основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности. ОПК-5.2. Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые	

			меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.	
		ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими	ОПК-6.1. Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему	Знать: – основные угрозы безопасности информации и модели нарушителя компьютерных систем; – систему нормативных правовых актов и стандартов по лицензированию в области защиты конфиденциальной информации. Уметь: – использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации; – разрабатывать модели угроз и модели нарушителя компьютерных систем;

		документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем. ОПК-6.2. разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.	– определить политику контроля доступа работников к информации ограниченного доступа; – формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; – применять отечественные и зарубежные стандарты в области компьютерной безопасности. Владеть: – навыками обеспечения использования правовых актов в своей профессиональной деятельности; – навыками защиты информации от утечки по техническим каналам.
		ОПК-7. Способен создавать программы	ОПК-7.1. Знает общие принципы построения, области и	Знать: – специфику создания низкоуровневого кода под

		на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	особенности применения языков программирования высокого и низкого уровня; язык программирования высокого и низкого уровня (объектно-ориентированное программирование); знает язык ассемблера персонального компьютера; базовые структуры данных; основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы; общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения. ОПК-7.2. Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого и низкого уровня алгоритмы решения типовых профессиональных задач; применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.3. Владеет навыками разработки, документирования, тестирования и отладки программ; навыками разработки алгоритмов решения типовых профессиональных задач.	современные процессоры. – современные средства разработки и анализа программного обеспечения на языках высокого уровня; – программные средства прикладного, системного и специального назначения, современные программные комплексы; – архитектуру и программный интерфейс современных операционных систем. Уметь: – проектировать программное обеспечение с учётом низкоуровневой специфики архитектуры современных процессоров; – составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные; – выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; – создавать код любой сложности под современные процессоры; – создавать прикладное и системное программное обеспечение для современных операционных систем. Владеть: – навыками реализации программного обеспечения любой сложности с использованием высокоуровневых и низкоуровневых языков программирования.

		ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-8.1. Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; средства и методы хранения и передачи и анализа конфиденциальной информации; основные методы научных исследований при разработке моделей безопасности компьютерных систем. ОПК-8.2. Умеет разрабатывать модели обнаружения угроз и модели обнаружения нарушителя безопасности компьютерных систем; применять методы научных исследований при проведении разработок моделей безопасности компьютерных систем. ОПК-8.3. Владеет способами моделирования безопасности компьютерных систем.	Знать: – виды и состав угроз информационной безопасности; – принципы и общие методы обеспечения информационной безопасности; – источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; – каналы и методы несанкционированного доступа к конфиденциальной информации; – состав объектов защиты информации. Уметь: – определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию; – определять возможные каналы и методы несанкционированного доступа; – принимать решения при выборе средств защиты информации на основе анализа угроз и рисков; – организовывать системное обеспечение защиты информации. Владеть: – навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий; – навыками разработки основных политик безопасности.
		ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами	ОПК-9.1. Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; возможности технических средств перехвата информации; методы защиты и средства обеспечения безопасности в	Знать: – основные понятия операционных систем и их защиты; – основные понятия, основные алгоритмы хранения и обработки данных ОС; – основные стандарты и алгоритмы передачи данных; – основные понятия защищенных операционных систем, баз данных и компьютерных сетей; – основные актуальные модели атак; – понятие защиты информации, системы защиты; – аппаратно-программные средства защиты информации: – средства обеспечения конфиденциальности данных; – средства аутентификации электронных данных и средства управления ключевой информацией;

		данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	операционных системах, компьютерных сетях и системах управления базами данных; методы предотвращения и обнаружения вторжений в операционных системах, компьютерных сетях и системах управления базами данных; технические каналы утечки информации. ОПК-9.2. Умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации; осуществлять меры противодействия нарушениям безопасности в операционных системах, компьютерных сетях и системах управления базами данных с использованием различных программных и аппаратных средств защиты. ОПК-9.3. Владеет методами и средствами технической защиты информации.	– цели и концептуальные основы защиты информации; – основные виды угроз безопасности информации и их классификацию. Уметь: – осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации; – оценивать угрозы безопасности клиентским ОС осуществлять проверку защищенности клиентских ОС; – осуществлять проверку защищенности серверных ОС; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – навыками настройки политики безопасности и учетных записей ОС оценки степени защищенности клиентских ОС; – навыками оценки степени безопасности ОС; – навыками администрирования протокольных средств обеспечения безопасности ОС; – навыками администрирования прав пользователей и аудита доступа к ресурсам ОС; – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети интернет.

		ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1. Знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; базовые понятия теории эллиптических кривых; типовые криптопротоколы, используемые в сетях связи; основные типы криптопротоколов и принципов их построения с использованием шифрсистем; основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты; основные типы криптографических методов защиты информации. ОПК-10.2. Умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях; исследовать и решать сравнения в кольцах вычетов; использовать достаточные условия простоты для построения больших простых чисел; оценивать теоретическую сложность применяемых алгоритмов; разворачивать инфраструктуру открытых ключей для решения	Знать: – основные понятия и классификацию средств криптографической защиты информации; – различия между стеганографией и криптографией; – основные методы симметричного шифрования; – классификацию методов симметричного шифрования; – основные свойства симметричных криптосистем; – понятие хеш-функции; – основные понятия, основные алгоритмы электронной цифровой подписи; – основные стандарты на алгоритмы цифровой подписи; – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. Уметь: – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной

			криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; проводить анализ криптографической стойкости хеш-функции, в том числе с использованием автоматизированных средств. ОПК-10.3. Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел; подходами к разработке и анализу безопасности криптографических протоколов; навыками использования типовых криптографических алгоритмов; подходами к разработке и анализу безопасности криптографических хеш-функции.	цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – основными методами симметричного шифрования; алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет. – основными методами симметричного шифрования; алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.
		ОПК-11. . Способен разрабатывать политики безопасности, политики управления	ОПК-11.1. Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; основные	Знать: – типовые модели политик безопасности КС, политик управления доступом и информационными потоками. Уметь: – самостоятельно разрабатывать новые и дорабатывать

		доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков. ОПК-11.2. Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками. ОПК-11.3. Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	типовые модели политик безопасности, управления доступом и информационными потоками, с учетом заданных требований. Владеть: – методами разработки моделей политик безопасности, управления доступом и информационными потоками.
		ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	ОПК-12.1. Знает принципы построения современных операционных систем и особенности их применения; принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей; основные	Знать: – общее устройство принципы работы современных операционных систем (ОС); – назначение и организацию основных служебных структур данных; – принципы работы механизмов защиты операционных систем семейств Windows и Linux. Уметь: – выполнять установку, настройку, обслуживание современных ОС. Владеть: – навыками настройки учетных записей ОС.

			принципы конфигурирования и администрирования операционных систем. ОПК-12.2. Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; применять основные методы программирования в выбранной операционной среде. ОПК-12.3.1 Владеет навыками системного программирования; навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.	
		ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ОПК-13.1. Знает средства и методы хранения и передачи аутентификационной информации; основные требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;	Знать: – цели и концептуальные основы защиты информации; – основные виды угроз безопасности информации и их классификацию; – программно-аппаратные средства защиты информации: – средства обеспечения конфиденциальности данных; – средства аутентификации электронных данных и средства управления ключевой информацией; – требования к криптографическим системам защиты информации; – понятие и виды криптографических атак. Уметь: – оценивать угрозы безопасности клиентским ОС; – проектировать и использовать системы электронной цифровой подписи; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных,

			основы физической защиты объектов информатизации. ОПК-13.2. Умеет формулировать и настраивать политику безопасности основных операционных систем; формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем; пользоваться нормативными документами в области технической защиты информации; анализировать и оценивать угрозы информационной безопасности объекта. ОПК-13.3. Владеет методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей эффективности технической защиты информации.	так и распределенных систем; – использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем; – использовать алгоритмы генерации, хранения и распределения ключей; – осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации; – осуществлять проверку защищенности клиентских ОС; – осуществлять проверку защищенности серверных ОС. Владеть: – основными методами администрирования и настройки ОС и сетей передачи; – алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети интернет; – методологией применения безопасных публичных служб; – методами управления ключами в системах с открытым ключом; – инструментами обеспечения безопасной работы в сети интернет.
		ОПК-14. Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации	ОПК-14.1. Знает характеристики и типы систем баз данных; основные языки запросов; физическую организацию баз данных и принципы (основы) их защиты; общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой	Знать: – характеристики и типы систем баз данных; – этапы проектирования баз данных; – физическую организацию баз данных; – основные модели структур данных; – способы организации файловых систем; – основные понятия о реляционной модели данных; – основные предложения языка запросов SQL; – области применения систем управления базами данных; – средства поддержания целостности в базах данных; – особенности управления данными в системах распределенной обработки; – порядок эксплуатации баз данных.

			доступности баз данных; особенности применения криптографической защиты в СУБД; этапы проектирования системы защиты в СУБД. ОПК-14.2. Умеет проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных; настраивать и применять современные системы управления базами данных; пользоваться средствами защиты, предоставляемыми СУБД; создавать дополнительные средства защиты баз данных; проводить анализ и оценивание механизмов защиты баз данных. ОПК-14.3. Владеет методикой и навыками составления запросов для поиска информации в базах данных; методикой и навыками использования средств защиты, предоставляемых СУБД.	Уметь: – разрабатывать программы на языках программирования четвертого поколения; – реализовывать на практике сложные структуры данных средствами реляционной СУБД; – использовать язык запросов SQL; – отображать предметную область на конкретную модель данных; – приводить в соответствие отношения при проектировании реляционной базы данных. Владеть: – навыками разработчика и администратора баз данных; – навыками поддержки и сопровождения баз данных; – навыками резервного копирования данных; – навыками обоснованного выбора инструментальных систем разработки баз данных; – навыками работы со средствами поддержания интерфейса с различными категориями пользователей СУБД; – навыками работы с системами управления базами данных на различных платформах.
		ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования	ОПК-15.1. Знает архитектуру основных типов современных компьютерных систем; принципы построения современных операционных систем и особенности их применения; основы организации и построения компьютерных сетей; эталонную модель взаимодействия открытых систем; функции, принципы действия и алгоритмы	Знать: – задачи и цели администрирования сетевой инфраструктуры организации; – основы функционирования сетевых протоколов и служб; – функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печати, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов; – принципы построения системы безопасности сетевой операционной системы; – задачи и цели администрирования беспроводной сетевой инфраструктуры;

			работы сетевого оборудования; основы организации и построения беспроводных компьютерных сетей. ОПК-15.2. Умеет реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования компьютерных сетей; реализовывать приложения для беспроводных сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования беспроводных компьютерных сетей. ОПК-15.3. Владеет навыками администрирования компьютерных сетей; навыками работы с сетевым оборудованием и сетевым программным обеспечением; навыками администрирования беспроводных компьютерных сетей; навыками работы с беспроводным сетевым оборудованием и сетевым программным обеспечением.	– основы функционирования беспроводных сетевых протоколов и служб; – принципы построения системы безопасности беспроводной сетевой инфраструктуры. Уметь: – проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации; – производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы; – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности; – проектировать беспроводную сетевую инфраструктуру в соответствии с потребностями построения информационной системы; – производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы; – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности. Владеть: – технологиями и навыками построения и администрирования службы каталогов информационной системы организации; – инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования; – методами и средствами аудита и мониторинга сетевых устройств и служб.; – технологиями и навыками построения и администрирования беспроводной сетевой инфраструктуры; – методами и средствами аудита и мониторинга беспроводных сетевых устройств и служб.
		ОПК-16. Способен проводить мониторинг	ОПК-16.1. Знает средства и методы хранения и передачи аутентификационной	Знать: – угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем;

		работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений; общие и специфические угрозы безопасности баз данных; основные критерии защищенности баз данных и методы оценивания механизмов защиты; механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных; особенности применения криптографической защиты в СУБД; этапы проектирования системы защиты в СУБД. ОПК-16.2. Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных	– типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем; – условия их осуществимости, возможные последствия, способы предотвращения; – угрозы и методы нарушения информационной безопасности БД; – типовые модели атак, направленных на преодоление защиты БД; – условия их осуществимости, возможные последствия, способы предотвращения. Уметь: – устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем; – устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем, БД. Владеть: – навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в сетях; – навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в БД.

			средств защиты; пользоваться средствами защиты, предоставляемыми СУБД; создавать дополнительные средства защиты баз данных; проводить анализ и оценивание механизмов защиты баз данных. ОПК-16.3. Владеет навыками настройки межсетевых экранов; методиками анализа сетевого трафика; методикой и навыками использования средств защиты, предоставляемых СУБД.	
		ОПК-17. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-17.1. Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира, выдающихся деятелей России. ОПК-17.2. Умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории России, опираясь на принципы историзма и научной объективности.	Знать: – основные этапы и закономерности исторического развития России. Уметь: – анализировать основные этапы и закономерности исторического развития , формулируя собственную точку зрения. Владеть: – приемами оценки исторических событий для формирования гражданской позиции.
		ОПК-1.1. Способен проводить анализ защищенности и осуществлять поиск	ОПК 1.1.1. Знает принципы построения защищенных компьютерных систем и сетей; требования основных стандартов	Знать: – российские и зарубежные стандарты в области информационной безопасности; – современные критерии и стандарты для анализа

		уязвимостей компьютерной системы	по оценке защищенности компьютерных систем и сетей; основные типы уязвимостей программного обеспечения; виды атак и механизмы их реализации в компьютерных системах; принципы построения защищенных компьютерных систем и сетей. ОПК 1.1.2. Умеет определять уровень защищенности и доверия программно-аппаратных средств защиты информации; классифицировать информационные системы по требованиям защиты информации; определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе; выполнять анализ компьютерной системы с целью определения уровня защищенности и доверия; проводить теоретические исследования уровней защищенности и доверия компьютерных систем и сетей; применять средства и методы анализа программных реализаций для поиска уязвимостей.	безопасности компьютерных систем; – особенности программирования шеллкодов; – методы исследования программного обеспечения без исходных кодов. Уметь: – оценивать соответствие проектной и эксплуатационной документации информационной системы на соответствие стандарту в области информационной безопасности; – применять современные критерии и стандарты для анализа безопасности компьютерных систем; – создавать шеллкоды для современных операционных системы под разные аппаратные платформы; – исследовать программное обеспечение без исходных кодов. Владеть: – практическими навыками оценки защищенности на соответствие стандартам информационной безопасности ЦБ РФ в области информационных систем, функционирующих в финансовой сфере; – практическими навыками работы с современными критериями и стандартами для анализа безопасности компьютерных систем; – навыками создания шеллкодов с учетом специфики различных сценариев использования; – навыками использования современных средств исследования программного обеспечения без исходных кодов.
		ОПК-1.2. Способен оценивать корректность программных реализаций алгоритмов защиты	ОПК 1.2.1. Знает основные средства и методы защиты программного обеспечения от анализа и нарушения целостности; основные программные методы защиты	Знать: – базовые методы функционирования вредоносного программного обеспечения; – методы защиты программного обеспечения от исследования, копирования, модификации; – форматы графических данных;

		информации	данных от несанкционированного доступа; теоретические основы устранения избыточности данных; основные алгоритмы кодирования данных и сжатия текстовой, графической, аудио- и видеоинформации; основные средства и методы защиты программного обеспечения от анализа и нарушения целостности. ОПК 1.2.2 Умеет проводить анализ программных средств, применяемых для контроля и защиты информации; проводить анализ программ и алгоритмов на предмет соответствия требованиям защиты информации; проводить анализ программ и алгоритмов сжатия данных на предмет соответствия требованиям защиты информации.	– дискретное преобразование Фурье; – вейвлетные преобразования; – кодирование источников информации; – словарные методы сжатия; – блочно-сортирующим сжатие. Уметь: – реализовывать базовые функциональные компоненты вредоносного программного обеспечения; – реализовывать методы защиты программного обеспечения от исследования с учетом специфики операционных систем, аппаратной платформы, используемой архитектуры; – разрабатывать и реализовывать алгоритмы кодирования и сжатия различных видов информации. Владеть: – навыками исследования вредоносного программного обеспечения с использованием современных инструментов анализа и собственных утилит; – навыками реализации методов защиты программного обеспечения от исследования и обхода этих методов; – методами оценки эффективности алгоритмов кодирования и сжатия различных видов информации.
		ОПК-1.3. Способен проводить тестирование и использовать средства верификации механизмов защиты информации	ОПК 1.3.1 Знает основные способы и средства верификации программ; основные способы тестирования средств защиты информации с использованием средств верификации программ; основные способы и средства верификации программ. ОПК 1.3.2 Умеет применять основные методы верификации программ и алгоритмов на предмет соответствия требованиям защиты информации.	Знать: – основы построения и реализации биометрических систем аутентификации, – основы тестирования и оценки надежности разработанных биометрических систем аутентификации. Уметь: – самостоятельно строить и анализировать алгоритмы, которые используются для построения биометрических систем аутентификации. Владеть: – навыками построения алгоритмов для биометрических систем аутентификации и проведения тестирования разработанных алгоритмов.

		ПК-1. Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; о порядке фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; о порядке проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о методах анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; о порядке подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем; о методах проведения расследования компьютерных преступлений, правонарушений и инцидентов; о методах анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов. ПК-1.2. Демонстрирует умения: применять нормативные и правовые акты при проведении	Знать: – основные принципы организации и использования всемирной сети Интернет; – нормативные и правовые акты в сфере информационной безопасности. Уметь: – эффективно использовать программные средства для поиска в сети Интернет (браузеры, специализированные библиотечные программы); – находить актуальную информацию в области компьютерной безопасности. Владеть: – навыками эффективного поиска в всемирной сети Интернет; – навыками фильтрации получаемой информации; – методами анализа источников информации.

			криминалистической экспертизы и криминалистического анализа; анализировать структуру механизма возникновения и обстоятельства события; определять причину и условия изменения программного обеспечения; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов. ПК-1.3. Имеет практический опыт (навыки): составления экспертного заключения; установления участников события, их роли, места, условий, при которых была создана, модифицирована или удалена информация; определения механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям; определения причин и условий изменения свойств исследуемой	

			информации; выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы; определения причин, целей и условий изменения свойств (состояния) программного обеспечения; индивидуального отождествления оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы.	
		ПК-2. Способен проводить мониторинг защищенности компьютерных систем и сетей	ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных мониторинга безопасности компьютерных систем и сетей; о порядке создания и структура отчета, создаваемого по результатам проверок; о способах обнаружения и нейтрализации последствий вторжений в компьютерные системы; о нормативных правовых актах в области защиты информации; о руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации. ПК-2.2. Демонстрирует умения: формализовывать задачу управления безопасностью компьютерных систем;	Знать: – общие положения интернета вещей; – стандарты и протоколы передачи данных в IoT; – практическую реализацию IoT; – принципы построения систем обнаружения компьютерных атак; – актуальные методы обработки данных мониторинга безопасности компьютерных систем и сетей; – нормативные правовые акты в области защиты информации; – архитектуру MPLS VPN; – базовые концепции MPLS; – модели Overlay VPN и Peer-to-Peer VPN; – назначение и распределение меток в сети MPLS; – основные концепции проектирования компьютерных сетей; – основы построения вычислительных сетей предприятия; – основы функционирования сетевых протоколов и служб; – понятие инфраструктуры корпоративной сети; – понятия и технологии корпоративных сетей, сетей LAN, сетей WAN; – принципы адресации и коммутации в корпоративной сети; – принципы использования IP-адресации в проекте компьютерной сети;

			применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет. ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.	– принципы построения системы безопасности сетевой операционной системы; – терминологию и архитектуру MPLS; – функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печа-ти, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов; – эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы. Уметь: – решать задачу управления безопасностью компьютерных систем; – применять инструментальные средства проведения мониторинга защищенности компьютерных систем; – применять методы анализа защищенности компьютерных систем и сетей; – структурировать аналитическую информацию для включения в отчет; – администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности; – внедрять списки доступа, позволяющие разрешать или отклонять трафик определенного типа; – настраивать протоколы маршрутизации устройств Cisco; – настраивать фильтрацию трафика с использованием списков контроля доступа; – описывать существующую компьютерную сеть, определять требования (влияние используемых приложений, требования пользователей, технические параметры и др.); – проводить испытания на прототипе сети WAN и устранять неполадки в корпоративных сетях; – проектировать простую компьютерную сеть с использованием технологий Cisco (разрабатывать схему IP-адресации, соответствующую требованиям локальной компьютерной сети; составлять список оборудования, соответствующего требованиям проекта локальной компьютерной сети; получать и обновлять программное обеспечение Cisco IOS для устройств Cisco); – получать и обновлять программное обеспечение Cisco IOS

				для устройств Cisco); – проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации; – производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы; – работать с протоколом VTP; – работать с протоколом связующего дерева STP; – разрабатывать и конфигурировать MPLS VPN; – разрабатывать технические и коммерческие предложения по созданию и модернизации компьютерной сети для комплекса зданий; – создавать каналы в корпоративной сети WAN; – создавать локальную сеть в соответствии с утвержденным проектом: настраивать коммутатор с поддержкой технологии VLAN и соединений между коммутаторами. Владеть: – навыками практической реализации IoT; – навыками анализа защищенности компьютерных систем с использованием сканеров безопасности; – навыками анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; – навыками составления отчетов по результатам проверок; – инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования; – методами и средствами аудита и мониторинга сетевых устройств и служб; – методикой анализа сетевого трафика; – навыками анализа требований заказчика и проектирования компьютерной сети; – навыками анализа, проектирования и настройки схем потоков трафика в компьютерной сети; – навыками мониторинга работы сети, обследования и модернизации сетевого оборудования; – навыками настройки коммутации в корпоративной сети;

				– навыками настройки адресации в сети на базе технологий VLSM, NAT и PAT; – навыками настройки механизмов фильтрации трафика на базе списков контроля доступа (ACL); – навыками настройки протоколов маршрутизации на базе протоколов RIPv2, EIGRP, OSPF; – навыками определения влияния приложений на проект сети; – навыками оценки качества и соответствия требованиям проекта сети; – навыками работы с виртуальными сетями VLAN; – навыками создания и настройки каналов корпоративной сети на базе технологий PPP, PAP, CHAP и Frame Relay; – навыками устранения проблем коммутации, связи, маршрутизации и конфигурации WAN; – навыками фильтрации, контроля и обеспечения безопасности сетевого трафика; – технологиями и навыками построения и администрирования службы каталогов информационной системы организации.
		ПК-3. Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в	Знать: - базовые программные алгоритмы и структуры данных. – роль эллиптических кривых в современных асимметричных шифрах; – формальные требования, предъявляемые к криптографическим эллиптическим кривым; – методы проникновения в компьютерные системы, используемые современным вредоносным программным обеспечением; – методы функционирования современного вредоносного программного обеспечения. Уметь: - применять базовые алгоритмы и структуры данных при решении прикладных задач. – анализировать криптографические эллиптические кривые на предмет их защищённости; – конструировать эллиптические кривые, обладающие заданными свойствами;

			операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.	– реализовывать современные атаки на компьютерные системы; – исследовать вредоносное программное обеспечение. Владеть: - навыками реализации базовых алгоритмов. – навыками разработки и конфигурирования программно-аппаратных средств криптографической защиты информации, основанных на криптографических эллиптических кривых; – инструментами проведения современных атак на компьютерные системы; – навыками использования инструментальных средств исследования вредоносного программного обеспечения.
		ПК-4. Способен разрабатывать требования и рекомендации к системам защиты информации в web-приложениях	ПК-4.1. Обладает знаниями о формировании политик безопасности компьютерных систем; о разработке технических заданий на создание средств защиты информации; об определении угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; о требованиях к защите информации компьютерной системы; о разработке руководящих документов по защите информации. ПК-4.2. Демонстрирует умения: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по	Знать: – математические модели безопасности компьютерных систем. Уметь: – проводить анализ математических моделей безопасности компьютерных систем. Владеть: – навыками разработки математических моделей безопасности компьютерных систем.

			безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; формировать политики безопасности компьютерных систем и сетей. ПК-4.3. Имеет практический опыт (навыки): использования средств защиты информации; использования нормативные правовые акты в области защиты информации; разработки руководящих документов по защите информации.	
		ПК-5. Способен управлять аналитическими работами и подразделениями	ПК-5.1. Обладает знаниями об управлении аналитическими ресурсами и компетенциями; об управлении процессами разработки и сопровождения требований к системам и управление качеством систем; об управлении инфраструктурой разработки и сопровождения требований к системе. ПК-5.2. Демонстрирует умения: разрабатывать технико-коммерческого предложения; разрабатывать методики выполнения аналитических работ; организовывать аналитические работы в ИТ-проекте; контролировать аналитические работы в ИТ-проекте. ПК-5.3. Имеет практический опыт (навыки): планирования аналитических работ в ИТ-	Знать: – информацию об аналитических ресурсами и компетенциях; – информацию об управлении процессами разработки и сопровождения требований к системам и управление качеством систем; – инфраструктуру разработки и сопровождения требований к системе. Уметь: – разрабатывать технико-коммерческие предложения; – разрабатывать методики выполнения аналитических работ; – организовывать аналитические работы в ИТ-проекте; – контролировать проведение аналитических работ в ИТ-проекте. Владеть: – навыками планирования аналитических работ в ИТ-проекте; – навыками составления отчетов об аналитических работах в ИТ-проекте; – навыками оценки квалификации сотрудников в ИТ-проекте.

			проекте; составления отчетов об аналитических работах в ИТ-проекте; оценки квалификации сотрудников в ИТ-проекте.	
ФТД Факультативные дисциплины				
ФТД.01	Технология программирования и работы на ЭВМ	ПК-5: Способен управлять аналитическими работами и подразделениями	ПК-5.1. Обладает знаниями об управлении аналитическими ресурсами и компетенциями; об управлении процессами разработки и сопровождения требований к системам и управление качеством систем; об управлении инфраструктурой разработки и сопровождения требований к системе. ПК-5.2. Демонстрирует умения: разрабатывать технико-коммерческого предложения; разрабатывать методики выполнения аналитических работ; организовывать аналитические работы в ИТ-проекте; контролировать аналитические работы в ИТ-проекте. ПК-5.3. Имеет практический опыт (навыки): планирования аналитических работ в ИТ-проекте; составления отчетов об аналитических работах в ИТ-проекте; оценки квалификации сотрудников в ИТ-проекте.	Знать: – определения архитектуры ЭВМ; механизмы организации вычислений; принципы взаимодействия структурных элементов ЭВМ; – процесс разработки и сопровождения требований к системам и управление качеством систем; – инфраструктуру разработки и сопровождения требований к системе. Уметь: – проводить сбор, обработку и анализ данных для определения ключевых свойств системы; – разрабатывать методики выполнения аналитических работ; – проводить исследование и анализ вычислительных систем. Владеть: – навыками описания модели вычислительной системы; – навыками классификации вычислительных систем; – навыками планирования аналитических работ в ИТ-проекте, составления отчетов об аналитических работах в ИТ-проекте.
ФТД.02	Линейные рекуррентные последовательности	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать	ОПК-3.1 Знает свойства основных дискретных структур: линейных рекуррентных последовательностей, графов, конечных автоматов, комбинаторных структур. ОПК-3.2 Умеет решать задачи периодичности и	Знать: – понятие ценности информации, защиты информации, системы защиты и данных; – понятие информации по уровню доступа; – конфиденциальность информации; – понятие конфиденциальной информации; – требования к криптографическим системам защиты информации;

		процедуры решения задач профессиональной деятельности	эквивалентности для линейных рекуррентных последовательностей и конечных автоматов. ОПК-3.2 Умеет применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач.	– способы реализации криптографических методов; – понятие и виды криптографических атак; – криптографический протокол; – криптографические методы защиты информации; – методы стеганографии; – классификация методов шифрования; – требования к современным шифрам; – цели и концептуальные основы защиты информации; – требования к криптографическим системам защиты информации; – понятие и виды криптографических атак. Уметь: – производить анализ типов информации в зависимости от порядка ее предоставления; – делать разбор методов обеспечения информационной безопасности; – подразделять основные средства защиты по видам деятельности. Владеть: – разработкой поточного симметрического шифрования.
		ОПК-10: Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Знает основные типы криптографических методов защиты информации. ОПК-10.2 Умеет проводить анализ криптографической стойкости хеш-функции, в том числе с использованием автоматизированных средств. ОПК-10.3 Владеет подходами к разработке и анализу безопасности криптографических хеш-функции.	Знать: – различия между стеганографией и криптографией; – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. Уметь: – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – основными методами симметричного шифрования;

				алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.