

**Матрица компетенций и планируемые результаты обучения по программе**

**10.05.01 Специализация № 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем" очная форма обучения 2023 г.н.**

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

	Б1.О.29	Б1	Защита в операционных системах	ОПК-9; ОПК-13
	Б1.О.30	Б1	Защита программ и данных	ОПК-13; ОПК-16
	Б1.О.31	Б1	Введение в специальность	ОПК-1; ПК-1
	Б1.О.32	Б1	Дисциплины(модули) специализации	ОПК-6.1; ОПК-6.2; ОПК-6.3
	Б1.О.32.01	Б1	Основы компьютерной криминалистики	ОПК-6.3
	Б1.О.32.02	Б1	Экспертиза вычислительной техники и компьютерных носителей информации	ОПК-6.2
	Б1.О.32.03	Б1	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	Тестирование компьютерных систем на проникновения	ПК-2
	Б1.В.02	Б1	Методы и стандарты оценки защищенности компьютерных систем	ПК-3
	Б1.В.03	Б1	Методы верификации	ПК-3
	Б1.В.ДВ.01	Б1	Элективные дисциплины (модули) 1	ПК-2
	Б1.В.ДВ.01.01	Б1	Защита IoT сетей	ПК-2
	Б1.В.ДВ.01.02	Б1	Сетевые технологии	ПК-2
	Б1.В.ДВ.02	Б1	Элективные дисциплины (модули) 2	ПК-3
	Б1.В.ДВ.02.01	Б1	Дополнительные главы криптографии	ПК-3
	Б1.В.ДВ.02.02	Б1	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	Философия	УК-1
	К.М.01.02	Б1	Сбор данных из открытых источников (научный семинар)	УК-1; ОПК-7
	К.М.01.03	Б1	Теоретико-числовые методы в криптографии	УК-1; ОПК-10
	К.М.01.04	Б1	Искусственный интеллект (научный семинар)	УК-1; ОПК-7; ОПК-8
	К.М.01.05	Б1	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	Правоведение	УК-1; УК-10
	К.М.02.02	Б1	Экономика	УК-9
	К.М.02.03	Б1	Языки программирования Python	УК-2; ОПК-7
	К.М.02.04	Б1	Параллельное программирование	УК-2; ОПК-7
	К.М.02.05	Б1	Методы программирования	УК-2; ОПК-7
	К.М.02.06	Б1	Web-программирование	УК-2; ОПК-7
	К.М.02.07	Б1	Технологии программирования	УК-2; ОПК-7
	К.М.02.08	Б1	Основы управленческой деятельности	УК-2; УК-3; УК-6
	К.М.02.09	Б1	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	История России	УК-5; ОПК-17
	К.М.03.02	Б1	Культура речи и деловое общение	УК-4
	К.М.03.03	Б1	Иностранный язык	УК-4
	К.М.03.04	Б1	Электроника и схемотехника	УК-4; ОПК-4
	К.М.03.05	Б1	Администрирование Windows	УК-4; ОПК-12
	К.М.03.06	Б1	Администрирование Linux и защита публичных служб	УК-4; ОПК-12
	К.М.03.07	Б1	Защита web-приложений	УК-4; ПК-4
	К.М.03.08	Б1	Основы российской государственности	УК-5
	К.М.04	К.М	Безопасность жизнедеятельности и здоровьесбережение	УК-7; УК-8
	К.М.04.01	Б1	Физическая культура и спорт	УК-7
	К.М.04.02	Б1	Безопасность жизнедеятельности	УК-8
	К.М.04.ДВ.01	Б1	Элективные дисциплины (модули) по физической культуре и спорту	
	К.М.04.ДВ.01.01	Б1	Прикладная физическая культура	УК-7
	К.М.04.ДВ.01.02	Б1	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	Учебная практика	ОПК-7; ПК-3
	Б2.О.01.01(У)	Б2	Учебно-лабораторный практикум	ОПК-7; ПК-3
	Б2.О.02	Б2	Производственная практика	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
	Б2.О.02.01(Н)	Б2	Научно-исследовательская работа	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
	Б2.О.02.02(П)	Б2	Технологическая практика	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5
	Б2.О.02.03(Пд)	Б2	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
	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»**

Дисциплина	Код и содержание компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
<b>Блок 1 Дисциплины (модули)</b>			
<b>Б1.О Обязательная часть</b>			
Б1.О.01	Алгебра	<p>ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности</p> <p>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.</p> <p>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.</p> <p>ОПК-3.3 Владеет 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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные понятия и методы алгебры.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– использовать алгебраические методы и модели для решения прикладных задач;</li> <li>– решать типовые задачи по алгебре,</li> <li>– выполнять операции с алгебраическими объектами.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– алгебраическими методами решения прикладных задач;</li> <li>– навыками решения типовых линейных уравнений;</li> <li>– навыками решения стандартных задач в векторных пространствах;</li> <li>– методами нахождения канонических форм линейных преобразований.</li> </ul>

			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 методы исследования числовых и функциональных рядов; ОПК-3.3 владеет навыками использования справочных материалов по математическому анализу.	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.
Б1.О.03	Геометрия	ОПК-3: Способен на основании совокупности математических методов разрабатывать,	ОПК-3.1. Знает основные задачи векторной алгебры и аналитической геометрии; возможности координатного метода для исследования различных геометрических объектов; основные	Знать: Для достижения ОПК-3.1: – основные задачи векторной алгебры и аналитической геометрии; возможности координатного метода для исследования различных геометрических объектов;

		<p>обосновывать и реализовывать процедуры решения задач профессиональной деятельности</p>	<p>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.</p>	<p>– 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.</p>
Б1.О.04	Теория вероятностей и математическая статистика	<p>ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности</p>	<p>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 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.</p>	<p>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 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</p>

				статистики.
Б1.О.05	Дискретная математика	ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	<p>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 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.</p> <p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные понятия и методы математической логики и теории алгоритмов;</li> <li>– основные понятия и методы дискретной математики.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– применять основные методы из математической логики и теории алгоритмов при решении задач;</li> <li>– применять основные алгоритмы и методы из теории графов и теории автоматов;</li> <li>– использовать полученные теоретические знания в самостоятельных исследованиях.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– методами решения прикладных задач.</li> </ul>

			<p>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.</p> <p>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.</p>	
Б1.О.06	Дифференциальные уравнения	<p>ОПК-3: Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности</p>	<p>ОПК-3.1. знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных; знает основные типы обыкновенных дифференциальных уравнений и методы их решения;</p> <p>ОПК-3.2. умеет обосновывать основные методы дифференциального исчисления функций одной и нескольких действительных переменных;</p>	<p>Знать: Обладает знаниями основных математических понятий и методов.</p> <p>Уметь: – использовать опыт применения математических методов для решения задач профессиональной деятельности.</p> <p>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;</p>

				– 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 реализовывать процедуры решения задач профессиональной деятельности	<p>ОПК-3.1. Знает 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.</p> <p>ОПК-3.2. Умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информация, пропускная способность); решать типовые задачи кодирования и декодирования; работать с научно-технической литературой по тематике дисциплины.</p> <p>ОПК-3.3. Владеет основами построения математических моделей текстовой информации и моделей систем передачи информации.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации;</li> <li>– основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума;</li> <li>– основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга);</li> <li>– понятие пропускной способности канала связи, прямую и обратную теоремы кодирования.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информация, пропускная способность);</li> <li>– решать типовые задачи кодирования и декодирования;</li> <li>– работать с научно-технической литературой по тематике дисциплины.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– основами построения математических моделей текстовой информации и моделей систем передачи информации;</li> <li>– навыками применения математического аппарата для решения прикладных теоретико-информационных задач.</li> </ul>
Б1.О.08	Аппаратные средства вычислительной техники	ОПК-4: Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования	ОПК-4.1. Знает архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов	<p>Знать:</p> <ul style="list-style-type: none"> <li>– физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники;</li> <li>– принципы работы и тенденции развития элементной базы, интерфейсов, процессоров и памяти, устройств</li> </ul>

		<p>микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности</p>	<p>электронной аппаратуры. 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.</p>	<p>ввода-вывода ЭВМ; – терминологию, уровни организации, способы классификации и стандартизации аппаратных средств вычислительной техники. 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.</p>
Б1.О.09	Физика	<p>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</p>	<p>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.</p>	<p>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 знаниями и практическими навыками, полученными в рамках изучения курса общей физики; – прогнозировать последствия физических процессов происходящих в профессиональной деятельности; – анализировать полученные экспериментальные данные.</p>

				<p>Владеть:</p> <ul style="list-style-type: none"> <li>– базовыми теоретическими знаниями и навыками лабораторных исследований в области физики;</li> <li>– навыком грамотного представления результатов исследований и навыком оформления отчетов по лабораторным работам.</li> </ul>
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	<p>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.</p> <p>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.</p>	<p>Знать:</p> <p>Для достижения индикатора ОПК-4.1: Знать</p> <ul style="list-style-type: none"> <li>– основные законы электричества и магнетизма;</li> <li>– основы теории колебаний и волн;</li> <li>– принципы работы элементов и функциональных узлов электронной аппаратуры;</li> <li>– знает архитектуру основных типов современных компьютерных систем;</li> <li>– структуру и принципы работы современных и перспективных микропроцессоров;</li> <li>– принципы работы элементов и функциональных узлов электронной аппаратуры.</li> </ul> <p>Уметь:</p> <p>Для достижения индикатора ОПК-4.2: Уметь</p> <ul style="list-style-type: none"> <li>– использовать математические модели физических явлений и процессов;</li> <li>– решать типовые прикладные физические задачи;</li> <li>– работать с современной элементной базой электронной аппаратуры;</li> <li>– определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– методами исследования физических явлений и процессов;</li> <li>– навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.</li> </ul>
Б1.О.11	Информатика	ОПК-2: Способен применять программные средства системного и	ОПК-2.1 Знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные современные тенденции развития информатики и вычислительной техники;</li> <li>– организацию создания программных средств;</li> </ul>

		<p>прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности</p>	<p>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.</p> <p>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.</p> <p>ОПК-2.3 Владеет средствами управления пользовательскими интерфейсами операционных систем.</p>	<p>– содержание различных этапов процесса разработки программных средств.</p> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– работать с простейшими аппаратами, приборами и схемами, понимать принципы их действия;</li> <li>– использовать существующие пакеты прикладных программ для решения конкретных задач.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– приемами и методами решения конкретных задач из областей технологии, с учетом требований по обеспечению информационной безопасности;</li> <li>– навыками работы с программно-техническими средствами;</li> <li>– основными принципами организации и взаимодействия программных компонентов.</li> </ul>
Б1.О.12	Языки программирования	<p>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</p>	<p>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).</p> <p>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;</p> <p>ОПК-7.3 Владеет навыками разработки, документирования, тестирования и отладки программ.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– программные средства прикладного, системного и специального назначения, современные программные комплексы;</li> <li>– современные средства разработки и анализа программного обеспечения на языках высокого уровня.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;</li> <li>– составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;</li> <li>– использовать языки программирования для решения задач.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками разработки программ на языке программирования высокого уровня;</li> <li>– навыками применения программных средств для</li> </ul>

				решения конкретных задач; – 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 программ	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 обеспечения; умеет разрабатывать и реализовывать на языке высокого и низкого уровня алгоритмы решения типовых профессиональных задач; умеет применять известные методы	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.

			<p>программирования и возможности базового языка программирования для решения типовых профессиональных задач.</p> <p>ОПК-7.3 Владеет навыками разработки алгоритмов решения типовых профессиональных задач; владеет навыками разработки, документирования, тестирования и отладки программ.</p>	
		<p>ОПК-13: Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности</p>	<p>ОПК-13.1 Знает общие принципы построения и использования современных языков программирования высокого и низкого уровня; современные технологии программирования; показатели качества программного обеспечения;</p> <p>ОПК-13.2 Умеет формализовать поставленную задачу, работать с интегрированными средами разработки программного обеспечения; разрабатывать эффективные алгоритмы и программы.</p> <p>ОПК-13.3 Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками разработки алгоритмов для решения типовых профессиональных задач.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– системную и программную архитектуру современных процессоров.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– создавать пользовательские программы;</li> <li>– создавать код режима ядра.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками использования инструментальных средств создания кода под современные операционные системы.</li> </ul>
Б1.О.15	Языки программирования Java	<p>ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения</p>	<p>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).</p> <p>ОПК-7.2 Умеет работать с интегрированной средой разработки</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– возможности языков программирования на примере Java;</li> <li>– области применения языка программирования Java;</li> <li>– основные особенности объектно-ориентированного подхода в программировании.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– работать в современных средствах разработки (IDE);</li> <li>– выделять объектную модель из поставленной</li> </ul>

		<p>профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ</p>	<p>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.</p>	<p>задачи. Владеть: – навыками разработки программного обеспечения на языке Java.</p>
Б1.О.16	Операционные системы	<p>ОПК-12: Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения</p>	<p>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 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.</p>	<p>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.</p>
Б1.О.17	Компьютерные сети	<p>ОПК-15: Способен администрировать компьютерные сети и контролировать корректность их функционирования</p>	<p>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</p>	<p>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.</p>

			<p>приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования компьютерных сетей.</p> <p>ОПК-15.3 Владеет навыками администрирования компьютерных сетей; навыками работы с сетевым оборудованием и сетевым программным обеспечением.</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>– проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации;</li> <li>– производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы;</li> <li>– администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– технологиями и навыками построения и администрирования службы каталогов информационной системы организации;</li> <li>– инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования;</li> <li>– методами и средствами аудита и мониторинга сетевых устройств и служб.</li> </ul>
Б1.О.18	Беспроводные сети	<p>ОПК-15: Способен администрировать компьютерные сети и контролировать корректность их функционирования</p>	<p>ОПК-15.1 Знает основы организации и построения беспроводных компьютерных сетей.</p> <p>ОПК-15.2 Умеет реализовывать приложения для беспроводных сетевых интерфейсов на нескольких современных программно-аппаратных платформах; осуществлять проектирование и оптимизацию функционирования беспроводных компьютерных сетей.</p> <p>ОПК-15.3 Владеет навыками администрирования беспроводных компьютерных сетей; навыками работы с беспроводным сетевым оборудованием и сетевым программным обеспечением.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– задачи и цели администрирования беспроводной сетевой инфраструктуры;</li> <li>– основы функционирования беспроводных сетевых протоколов и служб;</li> <li>– принципы построения системы безопасности беспроводной сетевой инфраструктуры.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проектировать беспроводную сетевую инфраструктуру в соответствии с потребностями построения информационной системы;</li> <li>– производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы;</li> <li>– администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– технологиями и навыками построения и администрирования беспроводной сетевой инфраструктуры;</li> </ul>

				– 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	<p>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.</p> <p>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.</p> <p>ОПК-14.3 Владеет методикой и навыками составления запросов для поиска информации в базах данных.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– характеристики и типы систем баз данных;</li> <li>– этапы проектирования баз данных;</li> <li>– физическую организацию баз данных;</li> <li>– основные модели структур данных;</li> <li>– способы организации файловых систем;</li> <li>– основные понятия о реляционной модели данных;</li> <li>– основные предложения языка запросов SQL;</li> <li>– области применения систем управления базами данных;</li> <li>– средства поддержания целостности в базах данных;</li> <li>– особенности управления данными в системах распределенной обработки;</li> <li>– порядок эксплуатации баз данных.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– разрабатывать программы на языках программирования четвертого поколения;</li> <li>– реализовывать на практике сложные структуры данных средствами реляционной СУБД;</li> <li>– использовать язык запросов SQL;</li> <li>– отображать предметную область на конкретную модель данных;</li> <li>– приводить в соответствие отношения при проектировании реляционной базы данных.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками разработчика и администратора баз данных;</li> <li>– навыками поддержки и сопровождения баз данных;</li> <li>– навыками резервного копирования данных;</li> <li>– навыками обоснованного выбора инструментальных систем разработки баз данных;</li> <li>– навыками работы со средствами поддержания интерфейса с различными категориями пользователей СУБД;</li> <li>– навыками работы с системами управления базами данных на различных платформах.</li> </ul>
Б1.О.20	Основы	ОПК-1: Способен	ОПК-1.1 Знает понятия информации,	Знать:

информационной безопасности	оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	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 информатизации.	– 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 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	УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	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. УК-10.3. Организует профессиональную среду, опираясь на этические и правовые нормы поведения, препятствующие проявлениям экстремизма, терроризма, формированию коррупционного поведения.	Знать: – этические и правовые нормы поведения; – содержание понятий «экстремизм», «терроризм», «коррупционное поведение»; основные формы их проявления и последствия; – основные термины и понятия гражданского права, используемые в антикоррупционном законодательстве; – практику применения действующего антикоррупционного законодательства. Уметь: – правильно толковать гражданско-правовые термины, используемые в антикоррупционном законодательстве; – разграничивать коррупционные и схожие некоррупционные явления в различных сферах жизни общества. Владеть: – навыками применения на практике антикоррупционного законодательства; – навыками пресечения коррупционного поведения; – навыками организации профессиональной среды, опираясь на этические и правовые нормы поведения, препятствующие проявлениям экстремизма, терроризма, формированию коррупционного поведения.
		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	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

	<p>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.</p> <p>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 компьютерной системы;</p>	<p>видам тайны и степеням конфиденциальности;</p> <ul style="list-style-type: none"> <li>– классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;</li> <li>– разрабатывать требования к системе защиты информации.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками работы с нормативными правовыми актами в области информационной безопасности;</li> <li>– навыками применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.</li> </ul>
--	---	--

		<p>формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.</p>	
	<p>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</p>	<p>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.</p> <p>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</p>	<p>Знать: – нормативные правовые акты в области защиты информации.</p> <p>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.</p> <p>Владеть: – навыками обеспечения использования правовых актов в своей профессиональной деятельности.</p>

			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 проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-8.1 Знает основные методы научных исследований при разработке моделей безопасности компьютерных 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.	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 состав конфиденциальной информации; – определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию; – определять возможные каналы и методы несанкционированного доступа;

				<ul style="list-style-type: none"> <li>– принимать решения при выборе средств защиты информации на основе анализа угроз и рисков;</li> <li>– организовывать системное обеспечение защиты информации.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий;</li> <li>– навыками разработки основных политик безопасности;</li> <li>– критериями, условиями и принципами отнесения информации к защищаемой;</li> <li>– методологией построения систем защиты автоматизированных систем.</li> </ul>
		<p>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</p>	<p>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 информационных потоков.</p> <p>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.</p> <p>ОПК-11.3 Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– типовые модели политик безопасности КС, политик управления доступом и информационными потоками.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности, управления доступом и информационными потоками, с учетом заданных требований.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– методами разработки моделей политик безопасности, управления доступом и информационными потоками.</li> </ul>

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	<p>ОПК-10.1 Знает основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты.</p> <p>ОПК-10.2 Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов.</p> <p>ОПК-10.3 Владеет навыками использования типовых криптографических алгоритмов.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные понятия и классификацию средств криптографической защиты информации;</li> <li>– различия между стеганографией и криптографией;</li> <li>– основные методы симметричного шифрования;</li> <li>– классификацию методов симметричного шифрования;</li> <li>– основные свойства симметричных криптосистем;</li> <li>– понятие хеш-функции;</li> <li>– основные понятия, основные алгоритмы электронной цифровой подписи;</li> <li>– основные стандарты на алгоритмы цифровой подписи;</li> <li>– основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– использовать блочные алгоритмы шифрования для формирования хеш-функции;</li> <li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать односторонние функции в целях построения криптосистем;</li> <li>– использовать алгоритмы генерации, хранения и распределения ключей;</li> <li>– проектировать и использовать системы электронной цифровой подписи;</li> <li>– применять на практике алгоритмы управления открытыми ключами.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– основными методами симметричного шифрования; алгоритмами формирования хеш-функций;</li> <li>– инструментами обеспечения безопасной работы в сети Интернет;</li> <li>– методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом;</li> <li>– технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.</li> </ul>
---------	---	--	--	---

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	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	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;

		<p>и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации</p>	<p>безопасности в операционных системах, компьютерных сетях и системах управления базами данных с использованием различных программных и аппаратных средств защиты.</p>	<p>– 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.</p>
		<p>ОПК-16: Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях</p>	<p>ОПК-16.1 Знает средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях ТСР/IP; основные протоколы идентификации и аутентификации абонентов сети; 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</p>	<p>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:          – 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.</p>

			различных программных и аппаратных средств защиты. ОПК-16.3 Владеет навыками настройки межсетевых экранов.	
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 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: – программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах 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 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,	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

			<p>предоставляемыми СУБД; создавать дополнительные средства защиты баз данных; проводить анализ и оценивание механизмов защиты баз данных.</p> <p>ОПК-16.3. Владеет методикой и навыками использования средств защиты, предоставляемых СУБД.</p>	<p>аппаратных средств, необходимых для реализации систем защиты информации в БД.</p>
Б1.О.28	<p>Защита информации от утечки по техническим каналам</p>	<p>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</p>	<p>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.</p> <p>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;</p>	<p>Знать:</p> <p>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</p> <p>Уметь:</p> <p>Для достижения индикатора ОПК-6.2: Уметь 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 для проектирования, разработки и оценивания защищенности компьютерной системы.</p> <p>Владеть:</p> <p>Для достижения индикатора ОПК-6.2: Владеть навыками защиты информации от утечки по техническим каналам</p>

			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.	
		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	ОПК-9.1 Знает методы защиты и средства обеспечения безопасности в операционных системах, компьютерных сетях и системах	Знать: – основные понятия операционных систем и их защиты; – основные понятия, основные алгоритмы хранения и

	<p>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</p>	<p>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.</p>	<p>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; – 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;</p>
--	--	---	---

				<ul style="list-style-type: none"> <li>– навыками оценки степени безопасности ОС;</li> <li>– навыками администрирования протокольных средств обеспечения безопасности ОС;</li> <li>– навыками администрирования прав пользователей и аудита доступа к ресурсам ОС;</li> <li>– основными методами администрирования и настройки ОС и сетей передачи;</li> <li>– алгоритмами формирования хеш-функций;</li> <li>– инструментами обеспечения безопасной работы в сети интернет;</li> <li>– методологией применения безопасных публичных служб;</li> <li>– методами управления ключами в системах с открытым ключом;</li> <li>– инструментами обеспечения безопасной работы в сети интернет.</li> </ul>
		<p>ОПК-13: Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности</p>	<p>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.</p> <p>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.</p> <p>ОПК-13.3 Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– цели и концептуальные основы защиты информации;</li> <li>– основные виды угроз безопасности информации и их классификацию;</li> <li>– программно-аппаратные средства защиты информации:</li> <li>– средства обеспечения конфиденциальности данных;</li> <li>– средства аутентификации электронных данных и средства управления ключевой информацией;</li> <li>– требования к криптографическим системам защиты информации;</li> <li>– понятие и виды криптографических атак.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– оценивать угрозы безопасности клиентским ОС;</li> <li>– проектировать и использовать системы электронной цифровой подписи;</li> <li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать алгоритмы генерации, хранения и</li> </ul>

				<p>распределения ключей;</p> <ul style="list-style-type: none"> <li>– осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;</li> <li>– осуществлять проверку защищенности клиентских ОС;</li> <li>– осуществлять проверку защищенности серверных ОС.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– основными методами администрирования и настройки ОС и сетей передачи;</li> <li>– алгоритмами формирования хеш-функций;</li> <li>– инструментами обеспечения безопасной работы в сети интернет;</li> <li>– методологией применения безопасных публичных служб;</li> <li>– методами управления ключами в системах с открытым ключом;</li> <li>– инструментами обеспечения безопасной работы в сети интернет.</li> </ul>
Б1.О.30	Защита программ и данных	<p>ОПК-13.Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности</p>	<p>ОПК-13.1. знает основные средства и методы защиты программного обеспечения от анализа; знает основные типы уязвимостей программного обеспечения;</p> <p>ОПК-13.2. умеет использовать программные средства анализа защиты компьютерных систем; умеет разрабатывать компоненты средств защиты информации.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– особенности программирования шеллкодов;</li> <li>– методы исследования программного обеспечения без исходных кодов.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– создавать шеллкоды для современных операционных системы под разные аппаратные платформы;</li> <li>– исследовать программное обеспечение без исходных кодов.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками создания шеллкодов с учетом специфики различных сценариев использования;</li> <li>– навыками использования современных средств исследования программного обеспечения без исходных кодов.</li> </ul>
		<p>ОПК-16.Способен проводить мониторинг работоспособности и</p>	<p>ОПК-16.1. знает средства мониторинга работоспособности средств защиты информации в компьютерных системах и сетях</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– базовые методы функционирования вредоносного программного обеспечения;</li> <li>– методы защиты программного обеспечения от</li> </ul>

		анализ эффективности 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.	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 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; 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.	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. 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,	ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов. ПК-1.2. Демонстрирует умения:	Знать: – свойства защищаемой информации, основы технологий поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов. Уметь:

		правонарушений и инцидентов	применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа. ПК-1.3. Имеет практический опыт (навыки): составления экспертного заключения.	– 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.
--	--	-----------------------------	--	--

**Дисциплины(модули) специализации**

Б1.О.32.01	Основы компьютерной криминалистики	ОПК-6.3.: Способен в качестве привлекаемого эксперта при проведении следственных и судебных действий применять нормативные правовые акты, методические документы, основы компьютерной криминалистики	ОПК-6.3.1. знает порядок проведения экспертизы 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	Знать: – порядок проведения экспертизы вычислительной техники 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.
------------	------------------------------------	--	---	--

			экспертизе компьютерных систем; фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов; умеет фиксировать и 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)	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.

			аппаратных средств в составе 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 проникновение	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;	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,
---------	---	--	--	--

			<p>применять инструментальные средства проведения мониторинга защищенности компьютерных систем; Применять методы анализа защищенности компьютерных систем и сетей; структурировать аналитическую информацию для включения в отчет.</p> <p>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.</p>	<p>антивирусного программного обеспечения и криптографических протоколов, применяемых для защиты компьютерных систем;</p> <p>– проводить оценку конфигурации средств защиты информации и давать рекомендации по ее корректировке.</p> <p>Владеть:</p> <p>– практическими навыками проведения тестирования компьютерных систем на проникновение и подготовки по их результатам соответствующих отчетов.</p>
Б1.В.02	Методы и стандарты оценки защищенности компьютерных систем	ПК-3: Способен проводить анализ безопасности компьютерных систем	<p>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.</p> <p>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.</p> <p>ПК-3.3. Имеет практический опыт</p>	<p>Знать:</p> <p>– российские и зарубежные стандарты в области информационной безопасности;</p> <p>– современные критерии и стандарты для анализа безопасности компьютерных систем.</p> <p>Уметь:</p> <p>– оценивать соответствие проектной и эксплуатационной документации информационной системы на соответствие стандарту в области информационной безопасности;</p> <p>– применять современные критерии и стандарты для анализа безопасности компьютерных систем.</p> <p>Владеть:</p> <p>– практическими навыками оценки защищенности на соответствие стандартам информационной безопасности ЦБ РФ в области информационных систем, функционирующих в финансовой сфере;</p> <p>– практическими навыками работы с современными критериями и стандартами для анализа безопасности компьютерных систем.</p>

			(навыки): выполнение анализа уязвимости 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 компьютерных систем.	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.

**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	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;
---------------	------------------	--	--	--

			<p>федеральных органов исполнительной власти по защите информации.</p> <p>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.</p> <p>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.</p>	<p>– применять методы анализа защищенности компьютерных систем и сетей;</p> <p>– структурировать аналитическую информацию для включения в отчет.</p> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками практической реализации IoT;</li> <li>– навыками анализа защищенности компьютерных систем с использованием сканеров безопасности;</li> <li>– навыками анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей;</li> <li>– навыками составления отчетов по результатам проверок.</li> </ul>
Б1.В.ДВ.01.02	Сетевые технологии	ПК-2: Способен проводить мониторинг защищенности компьютерных систем	<p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– архитектуру MPLS VPN;</li> <li>– базовые концепции MPLS;</li> <li>– модели Overlay VPN и Peer-to-Peer VPN;</li> <li>– назначение и распределение меток в сети MPLS;</li> <li>– основные концепции проектирования компьютерных сетей;</li> <li>– основы построения вычислительных сетей предприятия;</li> <li>– основы функционирования сетевых протоколов и служб;</li> <li>– понятие инфраструктуры корпоративной сети;</li> <li>– понятия и технологии корпоративных сетей, сетей LAN, сетей WAN;</li> <li>– принципы адресации и коммутации в</li> </ul>

			<p>федеральных органов исполнительной власти по защите информации.</p> <p>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.</p> <p>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.</p>	<p>корпоративной сети;</p> <ul style="list-style-type: none"> <li>– принципы использования IP-адресации в проекте компьютерной сети;</li> <li>– принципы построения системы безопасности сетевой операционной системы;</li> <li>– терминологию и архитектуру MPLS;</li> <li>– функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печатных служб, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов;</li> <li>– эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности;</li> <li>– внедрять списки доступа, позволяющие разрешать или отклонять трафик определенного типа;</li> <li>– настраивать фильтрацию трафика с использованием списков контроля доступа;</li> <li>– описывать существующую компьютерную сеть, определять требования (влияние используемых приложений, требования пользователей, технические параметры и др.);</li> <li>– проводить испытания на прототипе сети WAN и устранять неполадки в корпоративных сетях;</li> <li>– проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации;</li> <li>– производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы;</li> <li>– работать с протоколом VTP;</li> <li>– работать с протоколом связующего дерева STP;</li> <li>– разрабатывать и конфигурировать MPLS VPN;</li> <li>– разрабатывать технические и коммерческие предложения по созданию и модернизации компьютерной сети для комплекса зданий;</li> </ul>
--	--	--	---	--

				<ul style="list-style-type: none"> <li>– создавать каналы в корпоративной сети WAN;</li> <li>Владеть:</li> <li>– инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования;</li> <li>– методами и средствами аудита и мониторинга сетевых устройств и служб;</li> <li>– методикой анализа сетевого трафика;</li> <li>– навыками анализа требований заказчика и проектирования компьютерной сети;</li> <li>– навыками анализа, проектирования и настройки схем потоков трафика в компьютерной сети;</li> <li>– навыками мониторинга работы сети, обследования и модернизации сетевого оборудования;</li> <li>– навыками настройки коммутации в корпоративной сети;</li> <li>– навыками настройки адресации в сети на базе технологий VLSM, NAT и PAT;</li> <li>– навыками настройки механизмов фильтрации трафика на базе списков контроля доступа (ACL);</li> <li>– навыками настройки протоколов маршрутизации на базе протоколов RIPv2, EIGRP, OSPF;</li> <li>– навыками определения влияния приложений на проект сети;</li> <li>– навыками оценки качества и соответствия требованиям проекта сети;</li> <li>– навыками работы с виртуальными сетями VLAN;</li> <li>– навыками создания и настройки каналов корпоративной сети на базе технологий PPP, PAP, CHAP и Frame Relay;</li> <li>– навыками устранения проблем коммутации, связи, маршрутизации и конфигурации WAN;</li> <li>– навыками фильтрации, контроля и обеспечения безопасности сетевого трафика;</li> <li>– технологиями и навыками построения и администрирования службы каталогов информационной системы организации.</li> </ul>
--	--	--	--	---

**Б1.В.ДВ.02 Элективные дисциплины (модули) 2**

Б1.В.ДВ.02.01	Дополнительные главы криптографии	ПК-3: Способен проводить анализ	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в	Знать: – роль эллиптических кривых в современных
---------------	-----------------------------------	---------------------------------	--	---

		<p>безопасности компьютерных систем</p>	<p>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.</p>	<p>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-аппаратных средств криптографической защиты информации, основанных на криптографических эллиптических кривых.</p>
Б1.В.ДВ.02.02	Исследование вредоносного программного обеспечения	<p>ПК-3: Способен проводить анализ безопасности компьютерных систем</p>	<p>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</p>	<p>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.</p>

			(навыки): выполнение анализа уязвимости компьютерных систем.	
<b>Комплексные модули</b>				
<b>К.М.01 Системное и критическое мышление</b>				
К.М.01.01	Философия	УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать 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, – выработать 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, выработать 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	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;

		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, выработать 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 многочленов; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.	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.
К.М.01.04	Искусственный	УК-1: Способен	УК-1.1. Критически анализирует	Знать:

интеллект (научный семинар)	осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	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.	– 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 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. ОПК-8.2 Умеет разрабатывать модели обнаружения угроз и модели обнаружения нарушителя безопасности компьютерных систем.	Знать: – типовые модели политик безопасности компьютерных систем, 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.
К.М.01.05	Нечеткие модели и их приложения	УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать 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 ситуаций на основе системного подхода Уметь: Для достижения УК 1.2. уметь проводить анализ проблемных ситуаций 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
<b>К.М.02 Управление проектами</b>				
К.М.02.01	Правоведение	УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать 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: Для достижения УК-1.1. знать: основы права и законодательства России; Для достижения УК-1.2. знать: обстоятельства, при которых происходит зарождение, развитие и прекращение правовых отношений; Уметь: Для достижения УК-1.1. уметь: анализировать основные правовые акты; Для достижения УК-1.2. уметь: определять круг задач в рамках поставленных задач, исходя из действующих правовых норм; Владеть:

				<p>Для достижения УК-1.1. владеть: навыками анализа основные правовые акты;</p> <p>Для достижения УК-1.2. владеть: навыками определения круга задач в рамках поставленной цели и выбора оптимальных способы их решения, исходя из действующих правовых норм;</p>
		<p>УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности</p>	<p>УК-10.1. Имеет представление о содержании понятий «экстремизм», «терроризм», основных формах их проявления и последствиях.</p> <p>УК-10.2. Имеет представление о содержании понятия «коррупционное поведение», разграничивает коррупционные и схожие некоррупционные явления в различных сферах жизни общества.</p> <p>УК-10.3. Организует профессиональную среду, опираясь на этические и правовые нормы поведения, препятствующие проявлениям экстремизма, терроризма, формированию коррупционного поведения.</p>	<p>Знать:</p> <p>Для достижения УК-10.1. знать: содержание понятия «коррупционное поведение» и основных форм его проявления и последствия;</p> <p>Для достижения УК-10.2. знать: различия между коррупционными и некоррупционными явлениями;</p> <p>Для достижения УК-10.3. знать: о правовых формах нетерпимого отношения к коррупционному поведению.</p> <p>Уметь:</p> <p>Для достижения УК-10.1. уметь: различать формы проявления и определять последствия коррупционного поведения; Для достижения УК-10.2. уметь: разграничивать коррупционные и схожие некоррупционные явления в различных сферах жизни общества;</p> <p>Для достижения УК-10.3. уметь: демонстрировать нетерпимое отношение к коррупционному поведению.</p> <p>Владеть:</p> <p>Для достижения УК-10.1. владеть: навыками предотвращения коррупционного поведения;</p> <p>Для достижения УК-10.2. владеть: навыками путей определения коррупционного или некоррупционного характера явления в различных сферах жизни общества;</p> <p>Для достижения УК-10.3. владеть: навыками демонстрировать нетерпимое отношение к коррупционному поведению.</p>
К.М.02.02	Экономика	<p>УК-9: Способен принимать обоснованные экономические решения в различных</p>	<p>УК-9.1. Понимает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике.</p>	<p>Знать:</p> <p>Базовые экономические модели рыночной экономики.</p> <p>Уметь:</p> <p>Применять экономические знания в профессиональной деятельности.</p>

		областях жизнедеятельности	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.	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 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: – 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; – базовыми принципами и методологией построения информационных систем как систем, основанных на знаниях.
К.М.02.04	Параллельное программирование	УК-2: Способен управлять проектом	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает	Знать: – нормативно-правовую базу, регулирующую

		на всех этапах его жизненного цикла	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.	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 общие принципы построения, области и особенности применения языков программирования высокого уровня; знает язык программирования высокого уровня (объектно-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.	Знать: – современные языки и системы программирования; – программные средства прикладного, системного и специального назначения, современные программные комплексы. Уметь: – использовать языки программирования для решения 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	УК-2.1. Определяет этапы жизненного цикла проекта и выстраивает	Знать: – нормативно-правовую базу, регулирующую

		на всех этапах его жизненного цикла	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.	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.

		<p>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</p>	<p>ОПК-7.1 Знает общие принципы построения, области и особенности применения языков 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.</p>	<p>Знать: – программные средства прикладного, системного и специального назначения, современные программные 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.</p>
К.М.02.07	Технологии программирования	<p>УК-2: Способен управлять проектом на всех этапах его жизненного цикла</p>	<p>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.</p>	<p>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.</p>
		<p>ОПК-7: Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор</p>	<p>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</p>	<p>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</p>

		инструментария программирования и способов организации программ	типовых профессиональных задач. ОПК-7.3 Владеет навыками разработки алгоритмов решения типовых профессиональных задач.	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; – 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, выработывая 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 совершенствования на	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.	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:

		основе самооценки и образования в течение всей жизни	УК-6.3. Планирует результаты собственной деятельности с учетом необходимых ресурсов.	– 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 IT-проекте; контролировать аналитические работы в IT-проекте. ПК-5.3. Имеет практический опыт (навыки): планирования аналитических работ в IT-проекте; составления отчетов об аналитических работах в IT-проекте; оценки квалификации сотрудников в IT-проекте.	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.
<b>К.М.03 Коммуникация и межкультурное взаимодействие</b>				
К.М.03.01	История России	УК-5 Способен анализировать и учитывать	УК-5.1 Обладает необходимыми знаниями о разнообразии культур и об основных принципах межкультурного взаимодействия.	Знать: – обладает базовыми знаниями об основных закономерностях социально-исторического развития общества и его культурном многообразии.

		<p>разнообразие культур в процессе межкультурного взаимодействия</p>	<p>УК-5.2 Демонстрирует умение анализировать и использовать в профессиональной деятельности культурные и этические особенности среды.</p> <p>УК-5.3 Имеет навыки межкультурного взаимодействия при выполнении профессиональных задач.</p> <p>УК-5.4. Демонстрирует толерантное восприятие социальных и культурных различий, уважительное и бережное отношение к историческому наследию и культурным традициям.</p> <p>УК-5.5. Находит и использует необходимую для саморазвития и взаимодействия с другими людьми информацию о культурных особенностях и традициях различных социальных групп.</p> <p>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.</p> <p>УК-5.7. Сознательно выбирает ценностные ориентиры и гражданскую позицию; аргументировано обсуждает и решает проблемы мировоззренческого, общественного и личностного характера</p>	<p>Уметь:</p> <ul style="list-style-type: none"> <li>– демонстрирует умение понимать и толерантно воспринимать культурное многообразие общества в социально-историческом, этическом и философском контекстах.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– ориентируется в культурном разнообразии общества и соблюдает этические нормы поведения.</li> </ul>
		<p>ОПК-17: Способен анализировать основные этапы и закономерности исторического развития России, ее</p>	<p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные этапы и закономерности исторического развития России.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– анализировать основные этапы и закономерности исторического развития , формулируя собственную</li> </ul>

		<p>место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.</p>	<p>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.</p>	<p>точку зрения. Владеть: – приемами оценки исторических событий для формирования гражданской позиции.</p>
К.М.03.02	Культура речи и деловое общение	<p>УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p>	<p>УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах).</p>	<p>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 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 общезыковое 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</p>

				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; 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 иностранном языке.	Знать: Для достижения УК-4.1.: языковые средства и профессиональную терминологию по изученным темам, языковые нормы изучаемого языка. Для достижения УК-4.2.: современные коммуникативные технологии для академического и профессионального взаимодействия. Для достижения УК-4.3.: особенности и правила личной и профессиональной коммуникации устной и письменной коммуникации на иностранном языке. Уметь: Для достижения УК-4.1.: применять языковые средства и профессиональную терминологию по изученным темам, языковые нормы изучаемого языка. Для достижения УК-4.2.: использовать современные коммуникативные технологии для академического и профессионального взаимодействия. Для достижения УК-4.3.: применять особенности и правила личной и профессиональной коммуникации устной и письменной коммуникации на иностранном языке. Владеть: Для достижения УК-4.1.: навыками использования языковых средств и профессиональной терминологией по изученным темам, языковых норм изучаемого языка. Для достижения УК-4.2.: навыками использования современных коммуникативных технологий для академического и профессионального взаимодействия. Для достижения УК-4.3.: навыками использования особенностей и правил личной и профессиональной коммуникации устной и письменной коммуникации на иностранном языке.
К.М.03.04	Электроника и схемотехника	УК-4: Способен применять	УК-4.1. Обладает знаниями особенностей и правил личной и	Знать: Для достижения индикатора УК-4.1: Знать правила

		<p>современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p>	<p>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)</p>	<p>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</p>
		<p>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</p>	<p>ОПК-4.1. Знает принципы работы элементов и 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 комплексу документации.</p>	<p>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; 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:</p>

				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 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 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.
		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.	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;

			<p>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.</p> <p>ОПК-12.3 Владеет навыками системного программирования; навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.</p>	<p>– средства аутентификации электронных данных и средства управления ключевой информацией;</p> <p>– требования к криптографическим системам защиты информации;</p> <p>– понятиями компьютерной безопасности в рамках администрирования и защиты публичных служб Windows.</p> <p>Уметь:</p> <p>– использовать алгоритмы генерации, хранения и распределения ключей;</p> <p>– проектировать и использовать системы электронной цифровой подписи;</p> <p>– применять на практике алгоритмы управления открытыми ключами;</p> <p>– разрабатывать и конфигурировать программно-аппаратные средства защиты информации, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации.</p> <p>Владеть:</p> <p>– основными методами администрирования и настройки ОС и сетей передачи;</p> <p>– алгоритмами формирования хеш-функций;</p> <p>– инструментами обеспечения безопасной работы в сети интернет;</p> <p>– методологией применения безопасных публичных служб;</p> <p>– методами управления ключами в системах с открытым ключом;</p> <p>– инструментами обеспечения безопасной работы в сети интернет;</p> <p>– 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.</p>
К.М.03.06	Администрирование Linux и защита	УК-4: Способен применять	УК-4.1. Обладает знаниями особенностей и правил личной и	Знать: – основные термины и речевые обороты,

	<p>публичных служб</p>	<p>современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p>	<p>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).</p>	<p>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.</p>
		<p>ОПК-12: Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения</p>	<p>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</p>	<p>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.</p>

			к операционной системе с помощью системных вызовов.	
К.М.03.07	Защита web-приложений	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 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.
		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 безопасности компьютерных систем; выполнять	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

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

			<p>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</p>	<p>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 отношении 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</p>
--	--	--	--	--

				мировоззренческого, общественного и личного характера; осознанного выбора ценностных ориентиров и гражданской позиции; развитого чувства гражданственности и патриотизма, самостоятельного критического мышления; решения вызовы и проблемы мировоззренческого, общественного и личного характера.
<b>К.М.04 Безопасность жизнедеятельности и здоровьесбережение</b>				
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 для сохранения природной среды, обеспечения	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	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.

		устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	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.	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 физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.	Знать: Для достижения индикатора УК-7.1: знать здоровьесберегающие технологии и нормы здорового образа жизни. Для достижения индикатора УК-7.2: знать методы и средства физической культуры и спорта для сохранения и укрепления здоровья. Для достижения индикатора УК-7.3: знать принципы оптимального сочетания физической и умственной нагрузки для обеспечения работоспособности, процессов саморазвития и самообразования. Уметь: Для достижения индикатора УК-7.1: уметь осознанно выбирать здоровьесберегающие технологии для поддержания должного уровня физической и функциональной подготовленности. Для достижения индикатора УК-7.2: уметь применять методы и средства физической культуры и спорта для профессионально- личностного развития, физического самосовершенствования. Для достижения индикатора УК-7.3: уметь планировать свое рабочее время и время для саморазвития, формулировать цели личностного и профессионального развития, а также условия их достижения. Владеть:
-----------------	--	--	--	--

				<p>Для достижения индикатора УК-7.1: владеть навыками соблюдения норм здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности.</p> <p>Для достижения индикатора УК-7.2: владеть навыками соблюдения физической культуры для обеспечения полноценной социальной и профессиональной деятельности, сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности.</p> <p>Для достижения индикатора УК-7.3: владеть навыками саморазвития и управления своим временем для обеспечения полноценной социальной и профессиональной деятельности.</p>
К.М.04.ДВ.01.02	Оздоровительная физическая культура	УК-7: Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	<p>УК-7.1. Обладает знаниями здоровьесберегающих технологий для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.</p> <p>УК-7.2. Демонстрирует умения поддержания должного уровня физической подготовленности и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.</p> <p>УК-7.3- Имеет навыки поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.</p>	<p>Знать:</p> <p>Для достижения индикатора УК-7.1: знать здоровьесберегающие технологии и нормы здорового образа жизни.</p> <p>Для достижения индикатора УК-7.2: знать методы и средства физической культуры и спорта для сохранения и укрепления здоровья.</p> <p>Для достижения индикатора УК-7.3: знать принципы оптимального сочетания физической и умственной нагрузки для обеспечения работоспособности, процессов саморазвития и самообразования.</p> <p>Уметь:</p> <p>Для достижения индикатора УК-7.1: уметь осознанно выбирать здоровьесберегающие технологии для поддержания должного уровня физической и функциональной подготовленности.</p> <p>Для достижения индикатора УК-7.2: уметь применять методы и средства физической культуры и спорта для профессионально- личностного развития, физического самосовершенствования.</p> <p>Для достижения индикатора УК-7.3: уметь планировать свое рабочее время и время для саморазвития, формулировать цели личностного и профессионального развития, а также условия их достижения.</p>

				<p>Владеть:</p> <p>Для достижения индикатора УК-7.1: владеть навыками соблюдения норм здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности.</p> <p>Для достижения индикатора УК-7.2: владеть навыками соблюдения физической культуры для обеспечения полноценной социальной и профессиональной деятельности, сохранения и укрепления здоровья, психофизической подготовки и самоподготовки к будущей жизни и профессиональной деятельности.</p> <p>Для достижения индикатора УК-7.3: владеть навыками саморазвития и управления своим временем для обеспечения полноценной социальной и профессиональной деятельности.</p>
--	--	--	--	--

## 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 для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	<p>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.</p> <p>ОПК-7.2. Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого и низкого уровня</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>- основные понятия информатики и языков программирования;</li> <li>- язык программирования С и основы языка программирования С++.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- применять программные средства для решения математических задач;</li> <li>- использовать стандартные и сторонние библиотеки.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками реализации базовых математических алгоритмов;</li> <li>- навыками работы в интегрированной среде разработки (IDE) MS Visual Studio.</li> </ul>
---------------	-------------------------------	--	--	---

			<p>алгоритмы решения типовых профессиональных задач; применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.</p> <p>ОПК-7.3. Владеет навыками разработки, документирования, тестирования и отладки программ; навыками разработки алгоритмов решения типовых профессиональных задач.</p>	
		<p>ПК-3: Способен проводить анализ безопасности компьютерных систем</p>	<p>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.</p> <p>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.</p> <p>ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>- базовые программные алгоритмы и структуры данных.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- применять базовые алгоритмы и структуры данных при решении прикладных задач.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>- навыками реализации базовых алгоритмов.</li> </ul>
<b>Б2.О.02 Производственная практика</b>				
Б2.О.02.01(Н)	Научно-исследовательская работа	<p>ПК-1: Способен проводить экспертизы при расследовании компьютерных преступлений,</p>	<p>ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; о порядке фиксации и</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>- основные принципы организации и использования всемирной сети Интернет.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>- эффективно использовать программные средства</li> </ul>

		правонарушений и инцидентов	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 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	для поиска в сети Интернет (браузеры, специализированные библиотечные программы). Владеть: – навыками эффективного поиска в всемирной сети Интернет; – навыками фильтрации получаемой информации.
--	--	-----------------------------	---	---

			<p>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.</p> <p>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.</p>	
		<p>ПК-2: Способен проводить мониторинг защищенности</p>	<p>ПК-2.1. Обладает знаниями о принципах построения систем обнаружения компьютерных атак; о методах обработки данных</p>	<p>Знать: – базовые технологии информационной безопасности и математический аппарат лежащий в их основе.</p> <p>Уметь:</p>

		компьютерных систем	<p>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.</p> <p>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.</p> <p>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.</p>	<p>– грамотно использовать математический аппарат в решении прикладных задач.</p> <p>Владеть:</p> <p>– навыками научно-исследовательской работы, составления отчетной документации по ним.</p>
		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	<p>Знать:</p> <p>– стандарты в области безопасности компьютерных систем.</p> <p>Уметь:</p>

			<p>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.</p>	<p>– производить анализ безопасности компьютерных систем на соответствие стандартам. Владеть: – навыками оценки безопасности компьютерных систем на соответствие стандартам.</p>
		<p>ПК-4: Способен разрабатывать требования и рекомендации к системам защиты информации в web-приложениях</p>	<p>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 безопасности компьютерных систем; выполнять</p>	<p>Знать: – математические модели безопасности компьютерных систем. Уметь: – проводить анализ математических моделей безопасности компьютерных систем. Владеть: – навыками разработки математических моделей безопасности компьютерных систем.</p>

			<p>анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации; формировать политики безопасности компьютерных систем и сетей.</p> <p>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.</p>	
		ПК-5: Способен управлять аналитическими работами и подразделениями	<p>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.</p> <p>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.</p> <p>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.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– информацию об аналитических ресурсах и компетенциях;</li> <li>– информацию об управлении процессами разработки и сопровождения требований к системам и управление качеством систем;</li> <li>– инфраструктуру разработки и сопровождения требований к системе.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– разрабатывать технико-коммерческие предложения;</li> <li>– разрабатывать методики выполнения аналитических работ;</li> <li>– организовывать аналитические работы в ИТ-проекте;</li> <li>– контролировать проведение аналитических работ в ИТ-проекте.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками планирования аналитических работ в ИТ-проекте;</li> <li>– навыками составления отчетов об аналитических работах в ИТ-проекте;</li> <li>– навыками оценки квалификации сотрудников в ИТ-проекте.</li> </ul>
Б2.О.02.02(П)	Технологическая практика	ПК-1: Способен проводить экспертизы при расследовании	ПК-1.1. Обладает знаниями о технологиях поиска и анализа следов компьютерных преступлений,	<p>Знать:</p> <ul style="list-style-type: none"> <li>– нормативные и правовые акты в сфере информационной безопасности.</li> </ul>

		компьютерных преступлений, правонарушений и инцидентов	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 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	Уметь: – находить актуальную информацию в области компьютерной безопасности. Владеть: – методами поиска и анализа источников информации.
--	--	--	---	---

			<p>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.</p> <p>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.</p>	
		ПК-2: Способен проводить	ПК-2.1. Обладает знаниями о принципах построения систем	Знать: – современные научные методы исследований в

		<p>мониторинг защищенности компьютерных систем</p>	<p>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.</p> <p>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.</p> <p>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.</p>	<p>области информационной безопасности.</p> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– применять теоретические знания для решения исследовательских задач.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками проведения исследований в области защиты информации.</li> </ul>
		<p>ПК-3: Способен проводить анализ</p>	<p>ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– стандарты в области компьютерной безопасности.</li> </ul>

		<p>безопасности компьютерных систем</p>	<p>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.</p>	<p>Уметь:  – анализировать безопасность компьютерных систем.  Владеть:  – навыками оценки систем на соответствие стандартам безопасности.</p>
		<p>ПК-4: Способен разрабатывать требования и рекомендации к системам защиты информации в web-приложениях</p>	<p>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</p>	<p>Знать:  – математические модели безопасности компьютерных систем.  Уметь:  – производить анализ компьютерных систем.  Владеть:  – навыками разработки математических моделей безопасности.</p>

			<p>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.</p> <p>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.</p>	
		<p>ПК-5: Способен управлять аналитическими работами и подразделениями</p>	<p>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.</p> <p>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.</p> <p>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.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– современные методы защиты информации с использованием программно-аппаратных средств защиты информации.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проектировать комплексную систему защиты информации с использованием программно-аппаратных средств защиты информации.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками разработки и конфигурации программно-аппаратных средств защиты информации.</li> </ul>

Б2.О.02.03(Пд)	Преддипломная практика	ПК-1: Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	<p>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.</p> <p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– нормативные и правовые акты в сфере информационной безопасности.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– находить актуальную информацию в области компьютерной безопасности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– методами поиска и анализа источников информации.</li> </ul>
----------------	------------------------	--	---	---

			<p>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.</p> <p>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</p>	
--	--	--	---	--

			системы.	
		ПК-2: Способен проводить мониторинг защищенности компьютерных систем	<p>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.</p> <p>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.</p> <p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– современные научные методы исследований в области информационной безопасности.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– применять теоретические знания для решения исследовательских задач.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками проведения исследований в области защиты информации.</li> </ul>

			результатам проверок.	
		ПК-3: Способен проводить анализ безопасности компьютерных систем	<p>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.</p> <p>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.</p> <p>ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– стандарты в области компьютерной безопасности.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– анализировать безопасность компьютерных систем.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками оценки систем на соответствие стандартам безопасности.</li> </ul>
		ПК-4: Способен разрабатывать требования и рекомендации к системам защиты информации в web-приложениях	<p>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.</p> <p>ПК-4.2. Демонстрирует умения: анализировать компьютерную систему с целью определения необходимого</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– математические модели безопасности компьютерных систем.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– производить анализ компьютерных систем.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками разработки математических моделей безопасности.</li> </ul>

			<p>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.</p> <p>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.</p>	
		<p>ПК-5: Способен управлять аналитическими работами и подразделениями</p>	<p>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.</p> <p>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.</p> <p>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-</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– информацию об аналитических ресурсах и компетенциях;</li> <li>– информацию об управлении процессами разработки и сопровождения требований к системам и управление качеством систем;</li> <li>– инфраструктуру разработки и сопровождения требований к системе.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– разрабатывать технико-коммерческие предложения;</li> <li>– разрабатывать методики выполнения аналитических работ;</li> <li>– организовывать аналитические работы в ИТ-проекте;</li> <li>– контролировать проведение аналитических работ в ИТ-проекте.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками планирования аналитических работ в ИТ-проекте;</li> <li>– навыками составления отчетов об аналитических работах в ИТ-проекте;</li> <li>– навыками оценки квалификации сотрудников в ИТ-</li> </ul>

			проекте.	проекте.
<b>Б2.В Часть, формируемая участниками образовательных отношений</b>				
<b>Б3 Государственная итоговая аттестация</b>				
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 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 информатизации.	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 терминологии в области информационной безопасности.
		ОПК-2. Способен применять программные средства системного и прикладного назначения, 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	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:

			<p>структуры и принципы организации компьютерных сетей.</p> <p>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 интерфейсами операционных систем.</p> <p>ОПК-2.3. Владеет средствами управления пользовательскими интерфейсами операционных систем; навыками системного программирования.</p>	<p>– приемами и методами решения конкретных задач из областей технологии, с учетом требований по обеспечению информационной безопасности;</p> <p>– навыками работы с программно-техническими средствами;</p> <p>– основными принципами организации и взаимодействия программных компонентов.</p>
		<p>ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности</p>	<p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные математические методы.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– использовать математические методы и модели для решения задач профессиональной деятельности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– математическими методами решения прикладных задач профессиональной деятельности.</li> </ul>

		<p>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 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</p>	
--	--	---	--

			<p>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.</p> <p>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,</p>	
--	--	--	---	--

		<p>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</p>	
--	--	---	--

		<p>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.</p> <p>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</p>	
--	--	---	--

			<p>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.</p>	
		<p>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</p>	<p>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;</p>	<p>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 знаниями и практическими навыками для решения задач профессиональной деятельности;  – анализировать полученные экспериментальные данные.</p>

		<p>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.</p> <p>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.</p> <p>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</p>	<p>Владеть:</p> <ul style="list-style-type: none"> <li>– базовыми теоретическими знаниями и навыками лабораторных исследований в области физики;</li> <li>– навыком грамотного представления результатов исследований и навыком оформления отчетов по лабораторным работам.</li> </ul>
--	--	--	--

			<p>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.</p>	
		<p>ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации</p>	<p>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; 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</p>	<p>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.</p>

			<p>компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности.</p> <p>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</p>	
--	--	--	--	--

			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	<p>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.</p> <p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные угрозы безопасности информации и модели нарушителя компьютерных систем;</li> <li>– систему нормативных правовых актов и стандартов по лицензированию в области защиты конфиденциальной информации.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– использовать методы и средства обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации;</li> <li>– разрабатывать модели угроз и модели нарушителя компьютерных систем;</li> <li>– определить политику контроля доступа работников к информации ограниченного доступа;</li> <li>– формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации;</li> <li>– применять отечественные и зарубежные стандарты в области компьютерной безопасности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками обеспечения использования правовых актов в своей профессиональной деятельности;</li> <li>– навыками защиты информации от утечки по техническим каналам.</li> </ul>

			отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.	
		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	<p>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.</p> <p>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.</p> <p>ОПК-7.3. Владеет навыками разработки, документирования, тестирования и отладки программ; навыками разработки алгоритмов решения типовых профессиональных</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– специфику создания низкоуровневого кода под современные процессоры.</li> <li>– современные средства разработки и анализа программного обеспечения на языках высокого уровня;</li> <li>– программные средства прикладного, системного и специального назначения, современные программные комплексы;</li> <li>– архитектуру и программный интерфейс современных операционных систем.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проектировать программное обеспечение с учётом низкоуровневой специфики архитектуры современных процессоров;</li> <li>– составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;</li> <li>– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;</li> <li>– создавать код любой сложности под современные процессоры;</li> <li>– создавать прикладное и системное программное обеспечение для современных операционных систем.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками реализации программного обеспечения любой сложности с использованием высокоуровневых и низкоуровневых языков программирования.</li> </ul>

			задач.	
		ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	<p>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.</p> <p>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.</p> <p>ОПК-8.3. Владеет способами моделирования безопасности компьютерных систем.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– виды и состав угроз информационной безопасности;</li> <li>– принципы и общие методы обеспечения информационной безопасности;</li> <li>– источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;</li> <li>– каналы и методы несанкционированного доступа к конфиденциальной информации;</li> <li>– состав объектов защиты информации.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию;</li> <li>– определять возможные каналы и методы несанкционированного доступа;</li> <li>– принимать решения при выборе средств защиты информации на основе анализа угроз и рисков;</li> <li>– организовывать системное обеспечение защиты информации.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий;</li> <li>– навыками разработки основных политик безопасности.</li> </ul>
		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	<p>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 операционных системах, компьютерных сетях и системах управления базами данных; методы предотвращения и</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные понятия операционных систем и их защиты;</li> <li>– основные понятия, основные алгоритмы хранения и обработки данных ОС;</li> <li>– основные стандарты и алгоритмы передачи данных;</li> <li>– основные понятия защищенных операционных систем, баз данных и компьютерных сетей;</li> <li>– основные актуальные модели атак;</li> <li>– понятие защиты информации, системы защиты;</li> <li>– аппаратно-программные средства защиты информации;</li> <li>– средства обеспечения конфиденциальности данных;</li> <li>– средства аутентификации электронных данных и</li> </ul>

		<p>методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации</p>	<p>обнаружения вторжений в операционных системах, компьютерных сетях и системах управления базами данных; технические каналы утечки информации.</p> <p>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.</p> <p>ОПК-9.3. Владеет методами и средствами технической защиты информации.</p>	<p>средства управления ключевой информацией;</p> <ul style="list-style-type: none"> <li>– цели и концептуальные основы защиты информации;</li> <li>– основные виды угроз безопасности информации и их классификацию.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;</li> <li>– оценивать угрозы безопасности клиентским ОС</li> <li>– осуществлять проверку защищенности клиентских ОС;</li> <li>– осуществлять проверку защищенности серверных ОС;</li> <li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать алгоритмы генерации, хранения и распределения ключей;</li> <li>– проектировать и использовать системы электронной цифровой подписи;</li> <li>– применять на практике алгоритмы управления открытыми ключами.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками настройки политики безопасности и учетных записей ОС оценки степени защищенности клиентских ОС;</li> <li>– навыками оценки степени безопасности ОС;</li> <li>– навыками администрирования протокольных средств обеспечения безопасности ОС;</li> <li>– навыками администрирования прав пользователей и аудита доступа к ресурсам ОС;</li> <li>– основными методами администрирования и настройки ОС и сетей передачи;</li> <li>– алгоритмами формирования хеш-функций;</li> <li>– инструментами обеспечения безопасной работы в сети интернет;</li> </ul>
--	--	---	---	---

				<ul style="list-style-type: none"> <li>– методологией применения безопасных публичных служб;</li> <li>– методами управления ключами в системах с открытым ключом;</li> <li>– инструментами обеспечения безопасной работы в сети интернет.</li> </ul>
		<p>ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности</p>	<p>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.</p> <p>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;</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные понятия и классификацию средств криптографической защиты информации;</li> <li>– различия между стеганографией и криптографией;</li> <li>– основные методы симметричного шифрования;</li> <li>– классификацию методов симметричного шифрования;</li> <li>– основные свойства симметричных криптосистем;</li> <li>– понятие хеш-функции;</li> <li>– основные понятия, основные алгоритмы электронной цифровой подписи;</li> <li>– основные стандарты на алгоритмы цифровой подписи;</li> <li>– основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты.</li> <li>– основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– использовать блочные алгоритмы шифрования для формирования хеш-функции;</li> <li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать односторонние функции в целях построения криптосистем;</li> <li>– использовать алгоритмы генерации, хранения и распределения ключей;</li> <li>– проектировать и использовать системы электронной цифровой подписи;</li> <li>– применять на практике алгоритмы управления открытыми ключами.</li> <li>– использовать блочные алгоритмы шифрования для</li> </ul>

			<p>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.</p> <p>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.</p>	<p>формирования хеш-функции;</p> <ul style="list-style-type: none"> <li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать односторонние функции в целях построения криптосистем;</li> <li>– использовать алгоритмы генерации, хранения и распределения ключей;</li> <li>– проектировать и использовать системы электронной цифровой подписи;</li> <li>– применять на практике алгоритмы управления открытыми ключами.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– основными методами симметричного шифрования; алгоритмами формирования хеш-функций;</li> <li>– инструментами обеспечения безопасной работы в сети Интернет;</li> <li>– методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом;</li> <li>– технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.</li> <li>– основными методами симметричного шифрования; алгоритмами формирования хеш-функций;</li> <li>– инструментами обеспечения безопасной работы в сети Интернет;</li> <li>– методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом;</li> <li>– технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.</li> </ul>
		<p>ОПК-11. . Способен разрабатывать политики безопасности, политики управления</p>	<p>ОПК-11.1. Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; основные виды политик управления доступом и</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– типовые модели политик безопасности КС, политик управления доступом и информационными потоками.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– самостоятельно разрабатывать новые и</li> </ul>

		<p>доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации</p>	<p>информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.</p> <p>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.</p> <p>ОПК-11.3. Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.</p>	<p>дорабатывать типовые модели политик безопасности, управления доступом и информационными потоками, с учетом заданных требований.</p> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– методами разработки моделей политик безопасности, управления доступом и информационными потоками.</li> </ul>
		<p>ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения</p>	<p>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.</p> <p>ОПК-12.2. Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных,</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– общее устройство принципы работы современных операционных систем (ОС);</li> <li>– назначение и организацию основных служебных структур данных;</li> <li>– принципы работы механизмов защиты операционных систем семейств Windows и Linux.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– выполнять установку, настройку, обслуживание современных ОС.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками настройки учетных записей ОС.</li> </ul>

			<p>многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями; применять основные методы программирования в выбранной операционной среде.</p> <p>ОПК-12.3.1 Владеет навыками системного программирования; навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.</p>	
		<p>ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности</p>	<p>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; основы физической защиты объектов информатизации.</p> <p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– цели и концептуальные основы защиты информации;</li> <li>– основные виды угроз безопасности информации и их классификацию;</li> <li>– программно-аппаратные средства защиты информации;</li> <li>– средства обеспечения конфиденциальности данных;</li> <li>– средства аутентификации электронных данных и средства управления ключевой информацией;</li> <li>– требования к криптографическим системам защиты информации;</li> <li>– понятие и виды криптографических атак.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– оценивать угрозы безопасности клиентским ОС;</li> <li>– проектировать и использовать системы электронной цифровой подписи;</li> <li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать алгоритмы генерации, хранения и распределения ключей;</li> <li>– осуществлять рациональный выбор средств и методов защиты информации на объектах</li> </ul>

			<p>безопасности объекта.</p> <p>ОПК-13.3. Владеет методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей эффективности технической защиты информации.</p>	<p>информатизации;</p> <ul style="list-style-type: none"> <li>– осуществлять проверку защищенности клиентских ОС;</li> <li>– осуществлять проверку защищенности серверных ОС.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– основными методами администрирования и настройки ОС и сетей передачи;</li> <li>– алгоритмами формирования хеш-функций;</li> <li>– инструментами обеспечения безопасной работы в сети интернет;</li> <li>– методологией применения безопасных публичных служб;</li> <li>– методами управления ключами в системах с открытым ключом;</li> <li>– инструментами обеспечения безопасной работы в сети интернет.</li> </ul>
		<p>ОПК-14. Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации</p>	<p>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.</p> <p>ОПК-14.2. Умеет проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных;</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– характеристики и типы систем баз данных;</li> <li>– этапы проектирования баз данных;</li> <li>– физическую организацию баз данных;</li> <li>– основные модели структур данных;</li> <li>– способы организации файловых систем;</li> <li>– основные понятия о реляционной модели данных;</li> <li>– основные предложения языка запросов SQL;</li> <li>– области применения систем управления базами данных;</li> <li>– средства поддержания целостности в базах данных;</li> <li>– особенности управления данными в системах распределенной обработки;</li> <li>– порядок эксплуатации баз данных.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– разрабатывать программы на языках программирования четвертого поколения;</li> <li>– реализовывать на практике сложные структуры данных средствами реляционной СУБД;</li> <li>– использовать язык запросов SQL;</li> <li>– отображать предметную область на конкретную модель данных;</li> </ul>

			<p>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.</p> <p>ОПК-14.3. Владеет методикой и навыками составления запросов для поиска информации в базах данных; методикой и навыками использования средств защиты, предоставляемых СУБД.</p>	<p>– приводить в соответствие отношения при проектировании реляционной базы данных.</p> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками разработчика и администратора баз данных;</li> <li>– навыками поддержки и сопровождения баз данных;</li> <li>– навыками резервного копирования данных;</li> <li>– навыками обоснованного выбора инструментальных систем разработки баз данных;</li> <li>– навыками работы со средствами поддержания интерфейса с различными категориями пользователей СУБД;</li> <li>– навыками работы с системами управления базами данных на различных платформах.</li> </ul>
	<p>ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования</p>	<p>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; основы организации и построения беспроводных компьютерных сетей.</p> <p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– задачи и цели администрирования сетевой инфраструктуры организации;</li> <li>– основы функционирования сетевых протоколов и служб;</li> <li>– функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печати, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов;</li> <li>– принципы построения системы безопасности сетевой операционной системы;</li> <li>– задачи и цели администрирования беспроводной сетевой инфраструктуры;</li> <li>– основы функционирования беспроводных сетевых протоколов и служб;</li> <li>– принципы построения системы безопасности беспроводной сетевой инфраструктуры.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации;</li> <li>– производить установку и настройку операционных систем серверов и рабочих станций, настраивать</li> </ul>	

			<p>проектирование и оптимизацию функционирования беспроводных компьютерных сетей.</p> <p>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.</p>	<p>сетевое оборудование и сетевые протоколы;</p> <ul style="list-style-type: none"> <li>– администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности;</li> <li>– проектировать беспроводную сетевую инфраструктуру в соответствии с потребностями построения информационной системы;</li> <li>– производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы;</li> <li>– администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– технологиями и навыками построения и администрирования службы каталогов информационной системы организации;</li> <li>– инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования;</li> <li>– методами и средствами аудита и мониторинга сетевых устройств и служб.;</li> <li>– технологиями и навыками построения и администрирования беспроводной сетевой инфраструктуры;</li> <li>– методами и средствами аудита и мониторинга беспроводных сетевых устройств и служб.</li> </ul>
		<p>ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях</p>	<p>ОПК-16.1. Знает средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях ТСР/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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем;</li> <li>– типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем;</li> <li>– условия их осуществимости, возможные последствия, способы предотвращения;</li> <li>– угрозы и методы нарушения информационной безопасности БД;</li> <li>– типовые модели атак, направленных на преодоление защиты БД;</li> </ul>

			<p>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.</p> <p>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; пользоваться средствами защиты, предоставляемыми СУБД; создавать дополнительные средства защиты баз данных; проводить анализ и оценивание механизмов защиты баз данных.</p> <p>ОПК-16.3. Владеет навыками настройки межсетевых экранов; методиками анализа сетевого трафика; методикой и навыками использования средств защиты, предоставляемых СУБД.</p>	<p>– условия их осуществимости, возможные последствия, способы предотвращения.</p> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем;</li> <li>– устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем, БД.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в сетях;</li> <li>– навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в БД.</li> </ul>
		ОПК-17. Способен анализировать основные этапы и	ОПК-17.1. Знает основные закономерности исторического процесса, этапы исторического	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные этапы и закономерности исторического развития России.</li> </ul>

		закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	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.	Уметь: – анализировать основные этапы и закономерности исторического развития, формулируя собственную точку зрения. Владеть: – приемами оценки исторических событий для формирования гражданской позиции.
		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.
		ОПК-6.2.: Способен проводить экспертные исследования вычислительной техники и компьютерных носителей	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	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

		<p>информации в рамках информационно-аналитической и технической экспертизы компьютерных систем</p>	<p>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.</p> <p>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 компьютерной системы.</p>	<p>и носителей компьютерной информации;  – классификацию свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы;  – форматы хранения информации в анализируемой компьютерной системе.</p> <p>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.</p> <p>Владеть:  – навыками выполнения компьютерных экспертиз и исследований.</p>
		<p>ОПК-6.3.: Способен в качестве привлекаемого эксперта при проведении следственных и судебных действий применять нормативные правовые акты, методические документы, основы компьютерной</p>	<p>ОПК-6.3.1. знает порядок проведения экспертизы 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</p>	<p>Знать:  – порядок проведения экспертизы вычислительной техники 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</p>

		<p>криминалистики</p>	<p>технической экспертизе компьютерных систем; знает методику проведения работ по информационно-аналитической и технической экспертизе компьютерных систем.</p> <p>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 документировать следы компьютерных преступлений, правонарушений и инцидентов.</p>	<p>компьютерных систем.</p> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– подготавливать научно-технические экспертные заключения, по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем;</li> <li>– 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;</li> <li>– фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками самостоятельного проведения компьютерно-технических экспертиз и исследований.</li> </ul>
		<p>ПК-1. Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов</p>	<p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные принципы организации и использования всемирной сети Интернет;</li> <li>– нормативные и правовые акты в сфере информационной безопасности.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– эффективно использовать программные средства для поиска в сети Интернет (браузеры, специализированные библиотечные программы);</li> <li>– находить актуальную информацию в области компьютерной безопасности.</li> </ul> <p>Владеть:</p>

		<p>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.</p> <p>ПК-1.2. Демонстрирует умения:</p> <ul style="list-style-type: none"> <li>применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа;</li> <li>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,</li> </ul>	<ul style="list-style-type: none"> <li>– навыками эффективного поиска в всемирной сети Интернет;</li> <li>– навыками фильтрации получаемой информации;</li> <li>– методами анализа источников информации.</li> </ul>
--	--	--	--

			<p>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.</p>	
		<p>ПК-2. Способен проводить мониторинг защищенности компьютерных систем и сетей</p>	<p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– общие положения интернета вещей;</li> <li>– стандарты и протоколы передачи данных в IoT;</li> <li>– практическую реализацию IoT;</li> <li>– принципы построения систем обнаружения компьютерных атак;</li> <li>– актуальные методы обработки данных мониторинга безопасности компьютерных систем и сетей;</li> <li>– нормативные правовые акты в области защиты информации;</li> <li>– архитектуру MPLS VPN;</li> <li>– базовые концепции MPLS;</li> <li>– модели Overlay VPN и Peer-to-Peer VPN;</li> </ul>

			<p>руководящих и методических документах уполномоченных федеральных органов исполнительной власти по защите информации.</p> <p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> <li>– назначение и распределение меток в сети MPLS;</li> <li>– основные концепции проектирования компьютерных сетей;</li> <li>– основы построения вычислительных сетей предприятия;</li> <li>– основы функционирования сетевых протоколов и служб;</li> <li>– понятие инфраструктуры корпоративной сети;</li> <li>– понятия и технологии корпоративных сетей, сетей LAN, сетей WAN;</li> <li>– принципы адресации и коммутации в корпоративной сети;</li> <li>– принципы использования IP-адресации в проекте компьютерной сети;</li> <li>– принципы построения системы безопасности сетевой операционной системы;</li> <li>– терминологию и архитектуру MPLS;</li> <li>– функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печати, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов;</li> <li>– эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– решать задачу управления безопасностью компьютерных систем;</li> <li>– применять инструментальные средства проведения мониторинга защищенности компьютерных систем;</li> <li>– применять методы анализа защищенности компьютерных систем и сетей;</li> <li>– структурировать аналитическую информацию для включения в отчет;</li> <li>– администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности;</li> <li>– внедрять списки доступа, позволяющие разрешать или отклонять трафик определенного типа;–</li> </ul>
--	--	--	--	---

			<p>настраивать фильтрацию трафика с использованием списков контроля доступа;</p> <ul style="list-style-type: none"><li>– описывать существующую компьютерную сеть, определять требования (влияние используемых приложений, требования пользователей, технические параметры и др.);</li><li>– проводить испытания на прототипе сети WAN и устранять неполадки в корпоративных сетях;</li><li>– проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации;</li><li>– производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы;</li><li>– работать с протоколом VTP;</li><li>– работать с протоколом связующего дерева STP;</li><li>– разрабатывать и конфигурировать MPLS VPN;</li><li>– разрабатывать технические и коммерческие предложения по созданию и модернизации компьютерной сети для комплекса зданий;</li><li>– создавать каналы в корпоративной сети WAN;</li><li>– создавать локальную сеть в соответствии с утвержденным проектом: настраивать коммутатор с поддержкой технологии VLAN и соединений между коммутаторами.</li></ul> <p>Владеть:</p> <ul style="list-style-type: none"><li>– навыками практической реализации IoT;</li><li>– навыками анализа защищенности компьютерных систем с использованием сканеров безопасности;</li><li>– навыками анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей;</li><li>– навыками составления отчетов по результатам проверок;</li><li>– инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования;</li><li>– методами и средствами аудита и мониторинга</li></ul>
--	--	--	--

				<p>сетевых устройств и служб;</p> <ul style="list-style-type: none"> <li>– методикой анализа сетевого трафика;</li> <li>– навыками анализа требований заказчика и проектирования компьютерной сети;</li> <li>– навыками анализа, проектирования и настройки схем потоков трафика в компьютерной сети;</li> <li>– навыками мониторинга работы сети, обследования и модернизации сетевого оборудования;</li> <li>– навыками настройки коммутации в корпоративной сети;</li> <li>– навыками настройки адресации в сети на базе технологий VLSM, NAT и PAT;</li> <li>– навыками настройки механизмов фильтрации трафика на базе списков контроля доступа (ACL);</li> <li>– навыками настройки протоколов маршрутизации на базе протоколов RIPv2, EIGRP, OSPF;</li> <li>– навыками определения влияния приложений на проект сети;</li> <li>– навыками оценки качества и соответствия требованиям проекта сети;</li> <li>– навыками работы с виртуальными сетями VLAN;</li> <li>– навыками создания и настройки каналов корпоративной сети на базе технологий PPP, PAP, CHAP и Frame Relay;</li> <li>– навыками устранения проблем коммутации, связи, маршрутизации и конфигурации WAN;</li> <li>– навыками фильтрации, контроля и обеспечения безопасности сетевого трафика;</li> <li>– технологиями и навыками построения и администрирования службы каталогов информационной системы организации.</li> </ul>
		<p>ПК-3. Способен проводить анализ безопасности компьютерных систем</p>	<p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– базовые программные алгоритмы и структуры данных.</li> <li>– роль эллиптических кривых в современных асимметричных шифрах;</li> <li>– формальные требования, предъявляемые к криптографическим эллиптическим кривым;</li> <li>– методы проникновения в компьютерные системы, используемые современным вредоносным</li> </ul>

			<p>нормативных документов, а также их адекватности существующим рискам.</p> <p>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.</p> <p>ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.</p>	<p>программным обеспечением;</p> <ul style="list-style-type: none"> <li>– методы функционирования современного вредоносного программного обеспечения.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– применять базовые алгоритмы и структуры данных при решении прикладных задач.</li> <li>– анализировать криптографические эллиптические кривые на предмет их защищённости;</li> <li>– конструировать эллиптические кривые, обладающие заданными свойствами;</li> <li>– реализовывать современные атаки на компьютерные системы;</li> <li>– исследовать вредоносное программное обеспечение.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками реализации базовых алгоритмов.</li> <li>– навыками разработки и конфигурирования программно-аппаратных средств криптографической защиты информации, основанных на криптографических эллиптических кривых;</li> <li>– инструментами проведения современных атак на компьютерные системы;</li> <li>– навыками использования инструментальных средств исследования вредоносного программного обеспечения.</li> </ul>
		<p>ПК-4. Способен разрабатывать требования и рекомендации к системам защиты информации в web-приложениях</p>	<p>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.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– математические модели безопасности компьютерных систем.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проводить анализ математических моделей безопасности компьютерных систем.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками разработки математических моделей безопасности компьютерных систем.</li> </ul>

			<p>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.</p> <p>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.</p>	
		<p>ПК-5. Способен управлять аналитическими работами и подразделениями</p>	<p>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.</p> <p>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.</p> <p>ПК-5.3. Имеет практический опыт (навыки): планирования аналитических работ в ИТ-проекте;</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– информацию об аналитических ресурсах и компетенциях;</li> <li>– информацию об управлении процессами разработки и сопровождения требований к системам и управление качеством систем;</li> <li>– инфраструктуру разработки и сопровождения требований к системе.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– разрабатывать технико-коммерческие предложения;</li> <li>– разрабатывать методики выполнения аналитических работ;</li> <li>– организовывать аналитические работы в ИТ-проекте;</li> <li>– контролировать проведение аналитических работ в ИТ-проекте.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками планирования аналитических работ в ИТ-проекте;</li> </ul>

			составления отчетов об аналитических работах в ИТ-проекте; оценки квалификации сотрудников в ИТ-проекте.	– навыками составления отчетов об аналитических работах в ИТ-проекте; – навыками оценки квалификации сотрудников в ИТ-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, выработать 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, – выработать 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, выработывая 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.

		<p>УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия</p>	<p>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)</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные понятия и теоретические положения изучаемой дисциплины;</li> <li>– стиль делового общения, принципы деловой коммуникации в устной и письменной формах на государственном языке Российской Федерации;</li> <li>– правила профессиональной устной и письменной коммуникации для академического и профессионального взаимодействия;</li> <li>– современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– создавать устные и письменные тексты в соответствии с нормами современного русского литературного языка, используя лингвистические словари и справочную литературу;</li> <li>– строить деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации;</li> <li>– использовать современную измерительную литературу (в том числе на иностранном языке) при экспериментальном исследовании систем обработки информации.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– практическими навыками деловой коммуникации в устной и письменной формах на государственном языке Российской Федерации;</li> <li>– навыками организации работы (взаимодействия) проектной команды; навыками поиска информации, значимой для реализации проекта(для выполнения заданий).</li> <li>– навыками использования современной научно-технической информацией (в том числе на иностранном языке).</li> </ul>

		<p>УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия</p>	<p>УК-5.1 Обладает необходимыми знаниями о разнообразии культур и основных принципах межкультурного взаимодействия</p> <p>УК-5.2 Демонстрирует умение анализировать и использовать в профессиональной деятельности культурные и этические особенности среды.</p> <p>УК-5.3 Имеет навыки межкультурного взаимодействия при выполнении профессиональных задач</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– процессы жизненного цикла ПО, методы мониторинга и оценки качества процессов производственной деятельности, связанной с созданием и использованием информационных технологий.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– разрабатывать и реализовывать процессы жизненного цикла ПО;</li> <li>– реализовывать процессы управления качеством производственной деятельности, связанной с созданием и использованием информационных технологий;</li> <li>– осуществлять мониторинг и оценку качества процессов производственной деятельности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>использования методов и механизмов оценки и анализа функционирования средств ИТ;</li> <li>– навыки управления.</li> </ul>
		<p>УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни</p>	<p>УК-6.1. Применяет рефлексивные методы в процессе оценки разнообразных ресурсов, используемых для решения задач самоорганизации и саморазвития.</p> <p>УК-6.2. Определяет цели и приоритеты собственной деятельности и способы их достижения.</p> <p>УК-6.3. Планирует результаты собственной деятельности с учетом необходимых ресурсов.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– рефлексивные методы в процессе оценки разнообразных ресурсов, используемых для решения задач самоорганизации и саморазвития.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– определять цели и приоритеты собственной деятельности и способы их достижения.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками планирования результатов собственной деятельности с учетом необходимых ресурсов.</li> </ul>
		<p>УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и</p>	<p>УК-7.1. Обладает знаниями здоровьесберегающих технологий для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.</p> <p>УК-7.2. Демонстрирует умения</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– здоровьесберегающие технологии для поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– поддерживать должный уровень физической и функциональной подготовленности для обеспечения</li> </ul>

		<p>профессиональной деятельности</p>	<p>поддержания должного уровня физической подготовленности и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.</p> <p>УК-7.3. Имеет навыки поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности.</p>	<p>полноценной социальной и профессиональной деятельности</p> <p>Владеть:</p> <p>– навыками поддержания должного уровня физической и функциональной подготовленности для обеспечения полноценной социальной и профессиональной деятельности</p>
		<p>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</p>	<p>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.</p> <p>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.</p> <p>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.</p>	<p>Знать:</p> <p>– 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.</p> <p>Уметь:</p> <p>– обеспечивать создание и поддержание безопасных условий жизнедеятельности, оказания первой помощи, в том числе при возникновении чрезвычайных ситуаций.</p> <p>Владеть:</p> <p>– способами и технологиями создания и поддержания безопасных условий жизнедеятельности, алгоритм оказания первой помощи, в том числе при возникновении чрезвычайных ситуаций.</p>
		<p>УК-9. Способен использовать базовые дефектологические знания в социальной и</p>	<p>УК-9.1. Знает понятие инклюзивной компетентности, ее компоненты и структуру, особенности применения базовых дефектологических знаний в</p>	<p>Знать:</p> <p>– основные экономические категории и законы, принципы и методы экономического анализа.</p> <p>Уметь:</p>

		<p>профессиональной сферах.</p>	<p>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.</p>	<p>– 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.</p>
		<p>УК-10: Способен формировать нетерпимое отношение к коррупционному поведению</p>	<p>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.</p>	<p>Знать:  – понятие коррупции, коррупционного поведения;  – положения антикоррупционного законодательства.  Уметь:  – применять нормы антикоррупционного законодательства.  Владеть:  – навыками применения норм антикоррупционного законодательства.</p>
		<p>ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства</p>	<p>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</p>	<p>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</p>

			информационной безопасности для объекта информатизации.	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 назначения, 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 интерфейсами операционных систем.  ОПК-2.3. Владеет средствами управления пользовательскими интерфейсами операционных систем; навыками системного программирования.	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.
		ОПК-3. Способен на основании совокупности	ОПК-3.1. Знает основные задачи векторной алгебры и аналитической геометрии; возможности	Знать: – основные математические методы. Уметь:

		<p>математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности</p>	<p>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 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</p>	<p>– использовать математические методы и модели для решения задач профессиональной деятельности.  Владеть:  – математическими методами решения прикладных задач профессиональной деятельности.</p>
--	--	---	---	---

		<p>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;</p>	
--	--	--	--

		<p>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.</p> <p>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</p>	
--	--	---	--

		<p>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;</p>	
--	--	---	--

		<p>работать с научно-технической литературой по тематике дисциплины; использовать методы на основе теории нечетких множеств для решения прикладных задач.</p> <p>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-</p>	
--	--	---	--

			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	<p>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 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.</p> <p>ОПК-4.2. Умеет использовать математические модели физических явлений и процессов; решать типовые прикладные физические задачи; работать с современной элементной</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники;</li> <li>– базовые теоретические знания по физике;</li> <li>– смысл основных терминов и понятий физики.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– применять основные физические законы и модели для решения задач профессиональной деятельности;</li> <li>– пользоваться теоретическими знаниями и практическими навыками для решения задач профессиональной деятельности;</li> <li>– анализировать полученные экспериментальные данные.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– базовыми теоретическими знаниями и навыками лабораторных исследований в области физики;</li> <li>– навыком грамотного представления результатов исследований и навыком оформления отчетов по лабораторным работам.</li> </ul>

			<p>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.</p> <p>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.</p>	
		<p>ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие</p>	<p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– источники и классификацию угроз информационной безопасности;</li> <li>– основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– классифицировать защищаемую информацию по</li> </ul>

		<p>деятельность по защите информации</p>	<p>информационного общества в России; 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 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.</p> <p>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</p>	<p>видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.</p> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками работы с нормативными правовыми актами в области информационной безопасности;</li> <li>– навыками применения современной нормативной базы для построения системы организационных и программно-технических мер по выявлению и нейтрализации угроз безопасности компьютерных систем.</li> </ul>
--	--	--	--	---

			<p>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.</p>	
		<p>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</p>	<p>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</p>	<p>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;  – определить политику контроля доступа работников к информации ограниченного доступа;  – формулировать основные требования,</p>

		<p>Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем.</p> <p>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.</p>	<p>предъявляемые к физической защите объекта и пропускному режиму в организации;</p> <ul style="list-style-type: none"> <li>– применять отечественные и зарубежные стандарты в области компьютерной безопасности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками обеспечения использования правовых актов в своей профессиональной деятельности;</li> <li>– навыками защиты информации от утечки по техническим каналам.</li> </ul>
		<p>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</p>	<p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– специфику создания низкоуровневого кода под современные процессоры.</li> <li>– современные средства разработки и анализа программного обеспечения на языках высокого уровня;</li> <li>– программные средства прикладного, системного и специального назначения, современные программные комплексы;</li> <li>– архитектуру и программный интерфейс современных операционных систем.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проектировать программное обеспечение с учётом низкоуровневой специфики архитектуры</li> </ul>

		<p>программ</p>	<p>программного обеспечения.</p> <p>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.</p> <p>ОПК-7.3. Владеет навыками разработки, документирования, тестирования и отладки программ; навыками разработки алгоритмов решения типовых профессиональных задач.</p>	<p>современных процессоров;</p> <ul style="list-style-type: none"> <li>– составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;</li> <li>– выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;</li> <li>– создавать код любой сложности под современные процессоры;</li> <li>– создавать прикладное и системное программное обеспечение для современных операционных систем.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками реализации программного обеспечения любой сложности с использованием высокоуровневых и низкоуровневых языков программирования.</li> </ul>
		<p>ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей</p>	<p>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.</p> <p>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.</p> <p>ОПК-8.3. Владеет способами</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– виды и состав угроз информационной безопасности;</li> <li>– принципы и общие методы обеспечения информационной безопасности;</li> <li>– источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;</li> <li>– каналы и методы несанкционированного доступа к конфиденциальной информации;</li> <li>– состав объектов защиты информации.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию;</li> <li>– определять возможные каналы и методы несанкционированного доступа;</li> <li>– принимать решения при выборе средств защиты информации на основе анализа угроз и рисков;</li> <li>– организовывать системное обеспечение защиты информации.</li> </ul> <p>Владеть:</p>

			<p>моделирования безопасности компьютерных систем.</p>	<ul style="list-style-type: none"> <li>– навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий;</li> <li>– навыками разработки основных политик безопасности.</li> </ul>
		<p>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</p>	<p>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 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.</p> <p>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.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные понятия операционных систем и их защиты;</li> <li>– основные понятия, основные алгоритмы хранения и обработки данных ОС;</li> <li>– основные стандарты и алгоритмы передачи данных;</li> <li>– основные понятия защищенных операционных систем, баз данных и компьютерных сетей;</li> <li>– основные актуальные модели атак;</li> <li>– понятие защиты информации, системы защиты;</li> <li>– аппаратно-программные средства защиты информации;</li> <li>– средства обеспечения конфиденциальности данных;</li> <li>– средства аутентификации электронных данных и средства управления ключевой информацией;</li> <li>– цели и концептуальные основы защиты информации;</li> <li>– основные виды угроз безопасности информации и их классификацию.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;</li> <li>– оценивать угрозы безопасности клиентским ОС</li> <li>– осуществлять проверку защищенности клиентских ОС;</li> <li>– осуществлять проверку защищенности серверных ОС;</li> <li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать алгоритмы генерации, хранения и</li> </ul>

			<p>ОПК-9.3. Владеет методами и средствами технической защиты информации.</p>	<p>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.</p>
		<p>ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности</p>	<p>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,</p>	<p>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</p>

			<p>решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты; основные типы криптографических методов защиты информации.</p> <p>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 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.</p> <p>ОПК-10.3. Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов;</p>	<p>цифровой подписи и их возможные результаты. – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты.</p> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– использовать блочные алгоритмы шифрования для формирования хеш-функции;</li> <li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать односторонние функции в целях построения криптосистем;</li> <li>– использовать алгоритмы генерации, хранения и распределения ключей;</li> <li>– проектировать и использовать системы электронной цифровой подписи;</li> <li>– применять на практике алгоритмы управления открытыми ключами.</li> <li>– использовать блочные алгоритмы шифрования для формирования хеш-функции;</li> <li>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</li> <li>– использовать односторонние функции в целях построения криптосистем;</li> <li>– использовать алгоритмы генерации, хранения и распределения ключей;</li> <li>– проектировать и использовать системы электронной цифровой подписи;</li> <li>– применять на практике алгоритмы управления открытыми ключами.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– основными методами симметричного шифрования; алгоритмами формирования хеш-функций;</li> <li>– инструментами обеспечения безопасной работы в сети Интернет;</li> <li>– методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом;</li> </ul>
--	--	--	--	--

			<p>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.</p>	<p>– 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.</p>
		<p>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</p>	<p>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 информационных потоков.</p> <p>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.</p> <p>ОПК-11.3. Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и</p>	<p>Знать:  – типовые модели политик безопасности КС, политик управления доступом и информационными потоками.</p> <p>Уметь:  – самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности, управления доступом и информационными потоками, с учетом заданных требований.</p> <p>Владеть:  – методами разработки моделей политик безопасности, управления доступом и информационными потоками.</p>

			информационными потоками в компьютерных системах.	
		ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	<p>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.</p> <p>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.</p> <p>ОПК-12.3.1 Владеет навыками системного программирования; навыками разработки системных и прикладных программ, обращающихся к операционной системе с помощью системных вызовов.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– общее устройство принципы работы современных операционных систем (ОС);</li> <li>– назначение и организацию основных служебных структур данных;</li> <li>– принципы работы механизмов защиты операционных систем семейств Windows и Linux.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– выполнять установку, настройку, обслуживание современных ОС.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками настройки учетных записей ОС.</li> </ul>
		ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных	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	<p>Знать:</p> <ul style="list-style-type: none"> <li>– цели и концептуальные основы защиты информации;</li> <li>– основные виды угроз безопасности информации и их классификацию;</li> <li>– программно-аппаратные средства защиты информации;</li> </ul> <p>– средства обеспечения конфиденциальности данных;</p>

		<p>системах и проводить анализ их безопасности</p>	<p>информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; основы физической защиты объектов информатизации.</p> <p>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.</p> <p>ОПК-13.3. Владеет методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей эффективности технической защиты информации.</p>	<p>– средства аутентификации электронных данных и средства управления ключевой информацией;</p> <p>– требования к криптографическим системам защиты информации;</p> <p>– понятие и виды криптографических атак.</p> <p>Уметь:</p> <p>– оценивать угрозы безопасности клиентским ОС;</p> <p>– проектировать и использовать системы электронной цифровой подписи;</p> <p>– использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем;</p> <p>– использовать протоколы для защиты информации и обеспечения безопасности как локальных, так и распределенных систем;</p> <p>– использовать алгоритмы генерации, хранения и распределения ключей;</p> <p>– осуществлять рациональный выбор средств и методов защиты информации на объектах информатизации;</p> <p>– осуществлять проверку защищенности клиентских ОС;</p> <p>– осуществлять проверку защищенности серверных ОС.</p> <p>Владеть:</p> <p>– основными методами администрирования и настройки ОС и сетей передачи;</p> <p>– алгоритмами формирования хеш-функций;</p> <p>– инструментами обеспечения безопасной работы в сети интернет;</p> <p>– методологией применения безопасных публичных служб;</p> <p>– методами управления ключами в системах с открытым ключом;</p> <p>– инструментами обеспечения безопасной работы в сети интернет.</p>
		<p>ОПК-14. Способен проектировать базы данных,</p>	<p>ОПК-14.1. Знает характеристики и типы систем баз данных; основные языки запросов; физическую</p>	<p>Знать:</p> <p>– характеристики и типы систем баз данных;</p> <p>– этапы проектирования баз данных;</p>

		<p>администрировать системы управления базами данных в соответствии с требованиями по защите информации</p>	<p>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.</p> <p>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.</p> <p>ОПК-14.3. Владеет методикой и навыками составления запросов для поиска информации в базах данных; методикой и навыками использования средств защиты, предоставляемых СУБД.</p>	<ul style="list-style-type: none"> <li>– физическую организацию баз данных;</li> <li>– основные модели структур данных;</li> <li>– способы организации файловых систем;</li> <li>– основные понятия о реляционной модели данных;</li> <li>– основные предложения языка запросов SQL;</li> <li>– области применения систем управления базами данных;</li> <li>– средства поддержания целостности в базах данных;</li> <li>– особенности управления данными в системах распределенной обработки;</li> <li>– порядок эксплуатации баз данных.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– разрабатывать программы на языках программирования четвертого поколения;</li> <li>– реализовывать на практике сложные структуры данных средствами реляционной СУБД;</li> <li>– использовать язык запросов SQL;</li> <li>– отображать предметную область на конкретную модель данных;</li> <li>– приводить в соответствие отношения при проектировании реляционной базы данных.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками разработчика и администратора баз данных;</li> <li>– навыками поддержки и сопровождения баз данных;</li> <li>– навыками резервного копирования данных;</li> <li>– навыками обоснованного выбора инструментальных систем разработки баз данных;</li> <li>– навыками работы со средствами поддержания интерфейса с различными категориями пользователей СУБД;</li> <li>– навыками работы с системами управления базами данных на различных платформах.</li> </ul>
		<p>ОПК-15. Способен администрировать компьютерные сети и контролировать их корректность их функционирования</p>	<p>ОПК-15.1. Знает архитектуру основных типов современных компьютерных систем; принципы построения современных операционных систем и особенности их применения; основы организации и</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– задачи и цели администрирования сетевой инфраструктуры организации;</li> <li>– основы функционирования сетевых протоколов и служб;</li> <li>– функции управления информационными ресурсами</li> </ul>

			<p>построения компьютерных сетей; эталонную модель взаимодействия открытых систем; функции, принципы действия и алгоритмы работы сетевого оборудования; основы организации и построения беспроводных компьютерных сетей.</p> <p>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.</p> <p>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.</p>	<p>(файловыми и дисковыми ресурсами), ресурсами печати, службами маршрутизации, удалённого доступа, резервного копирования, службой терминалов;</p> <ul style="list-style-type: none"> <li>– принципы построения системы безопасности сетевой операционной системы;</li> <li>– задачи и цели администрирования беспроводной сетевой инфраструктуры;</li> <li>– основы функционирования беспроводных сетевых протоколов и служб;</li> <li>– принципы построения системы безопасности беспроводной сетевой инфраструктуры.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации;</li> <li>– производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы;</li> <li>– администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности;</li> <li>– проектировать беспроводную сетевую инфраструктуру в соответствии с потребностями построения информационной системы;</li> <li>– производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы;</li> <li>– администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– технологиями и навыками построения и администрирования службы каталогов информационной системы организации;</li> <li>– инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования;</li> </ul>
--	--	--	--	--

				<ul style="list-style-type: none"> <li>– методами и средствами аудита и мониторинга сетевых устройств и служб.;</li> <li>– технологиями и навыками построения и администрирования беспроводной сетевой инфраструктуры;</li> <li>– методами и средствами аудита и мониторинга беспроводных сетевых устройств и служб.</li> </ul>
		<p>ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях</p>	<p>ОПК-16.1. Знает средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях ТСР/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.</p> <p>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</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем;</li> <li>– типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем;</li> <li>– условия их осуществимости, возможные последствия, способы предотвращения;</li> <li>– угрозы и методы нарушения информационной безопасности БД;</li> <li>– типовые модели атак, направленных на преодоление защиты БД;</li> <li>– условия их осуществимости, возможные последствия, способы предотвращения.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем;</li> <li>– устанавливать и обслуживать современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем, БД.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в сетях;</li> <li>– навыками применения основных программных и аппаратных средств, необходимых для реализации систем защиты информации в БД.</li> </ul>

			<p>безопасности с 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.</p> <p>ОПК-16.3. Владеет навыками настройки межсетевых экранов; методиками анализа сетевого трафика; методикой и навыками использования средств защиты, предоставляемых СУБД.</p>	
		<p>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</p>	<p>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.</p> <p>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.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные этапы и закономерности исторического развития России.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– анализировать основные этапы и закономерности исторического развития, формулируя собственную точку зрения.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– приемами оценки исторических событий для формирования гражданской позиции.</li> </ul>
		<p>ОПК-6.1.: Способен использовать технологии поиска, фиксации и документирования</p>	<p>ОПК-6.1.1. Знает основные этапы и методы проведения расследования компьютерных преступлений, правонарушений и инцидентов; знает методы и средства сбора и</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные этапы и методы проведения расследования компьютерных преступлений, правонарушений и инцидентов;</li> <li>– методы и средства сбора и обращения с</li> </ul>

		<p>следов компьютерных преступлений, правонарушений и инцидентов;</p>	<p>обращения с доказательными данными.</p> <p>ОПК-6.1.2. Умеет определять причины, цели и условия изменения свойств (состояния) программного обеспечения;</p> <p>умеет обращаться со свободно распространяемыми инструментальными средствами сбора, анализа и хранения доказательных данных.</p>	<p>доказательными данными.</p> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– определять причины, цели и условия изменения свойств (состояния) программного обеспечения;</li> <li>– обращаться со свободно распространяемыми инструментальными средствами сбора, анализа и хранения доказательных данных.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– способами правильного установления, фиксации и оценки следов компьютерных преступлений и инцидентов.</li> </ul>
		<p>ОПК-6.2.: Способен проводить экспертные исследования вычислительной техники и компьютерных носителей информации в рамках информационно-аналитической и технической экспертизы компьютерных систем</p>	<p>ОПК-6.2.1. Знает нормативные и правовые акты, регламентирующие проведение компьютерно-технических экспертиз;</p> <p>знает современные методы и средства проведения экспертиз вычислительной техники и носителей компьютерной информации;</p> <p>знает основные типы экспертиз вычислительной техники и носителей компьютерной информации;</p> <p>знает классификацию свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы;</p> <p>знает форматы хранения информации в анализируемой компьютерной системе.</p> <p>ОПК-6.2.2. Умеет обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации;</p> <p>умеет определять свойства аппаратных средств в составе компьютерной системы и их фактического и первоначального</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– нормативные и правовые акты, регламентирующие проведение компьютерно-технических экспертиз;</li> <li>– современные методы и средства проведения экспертиз вычислительной техники и носителей компьютерной информации;</li> <li>– основные типы экспертиз вычислительной техники и носителей компьютерной информации;</li> <li>– классификацию свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы;</li> <li>– форматы хранения информации в анализируемой компьютерной системе.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации;</li> <li>– определять свойства аппаратных средств в составе компьютерной системы и их фактического и первоначального состояния;</li> <li>– анализировать структуру механизма изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками выполнения компьютерных экспертиз и исследований.</li> </ul>

			состояния; умеет анализировать структуру механизма изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы.	
		ОПК-6.3.: Способен в качестве привлекаемого эксперта при проведении следственных и судебных действий применять нормативные правовые акты, методические документы, основы компьютерной криминалистики	<p>ОПК-6.3.1. знает порядок проведения экспертизы 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.</p> <p>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,</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов;</li> <li>– виды преступлений в сфере компьютерной информации;</li> <li>– основные требования, предъявляемые к составу и оформлению научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем;</li> <li>– методику проведения работ по информационно-аналитической и технической экспертизе компьютерных систем.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– подготавливать научно-технические экспертные заключения, по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем;</li> <li>– 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;</li> <li>– фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками самостоятельного проведения компьютерно-технических экспертиз и исследований.</li> </ul>

			<p>правонарушений и инцидентов; умеет фиксировать и документировать следы компьютерных преступлений, правонарушений и инцидентов.</p>	
		<p>ПК-1. Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов</p>	<p>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.</p> <p>ПК-1.2. Демонстрирует умения: применять нормативные и правовые акты при проведении</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– основные принципы организации и использования всемирной сети Интернет;</li> <li>– нормативные и правовые акты в сфере информационной безопасности.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– эффективно использовать программные средства для поиска в сети Интернет (браузеры, специализированные библиотечные программы);</li> <li>– находить актуальную информацию в области компьютерной безопасности.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками эффективного поиска в всемирной сети Интернет;</li> <li>– навыками фильтрации получаемой информации;</li> <li>– методами анализа источников информации.</li> </ul>

		<p>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.</p> <p>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)</p>	
--	--	---	--

			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	<p>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.</p> <p>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.</p> <p>ПК-2.3. Имеет практический опыт (навыки): выполнение анализа защищенности компьютерных систем с использованием сканеров безопасности; выполнение анализа защищенности сетевых сервисов с</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– общие положения интернета вещей;</li> <li>– стандарты и протоколы передачи данных в IoT;</li> <li>– практическую реализацию IoT;</li> <li>– принципы построения систем обнаружения компьютерных атак;</li> <li>– актуальные методы обработки данных мониторинга безопасности компьютерных систем и сетей;</li> <li>– нормативные правовые акты в области защиты информации;</li> <li>– архитектуру MPLS VPN;</li> <li>– базовые концепции MPLS;</li> <li>– модели Overlay VPN и Peer-to-Peer VPN;</li> <li>– назначение и распределение меток в сети MPLS;</li> <li>– основные концепции проектирования компьютерных сетей;</li> <li>– основы построения вычислительных сетей предприятия;</li> <li>– основы функционирования сетевых протоколов и служб;</li> <li>– понятие инфраструктуры корпоративной сети;</li> <li>– понятия и технологии корпоративных сетей, сетей LAN, сетей WAN;</li> <li>– принципы адресации и коммутации в корпоративной сети;</li> <li>– принципы использования IP-адресации в проекте компьютерной сети;</li> <li>– принципы построения системы безопасности сетевой операционной системы;</li> <li>– терминологию и архитектуру MPLS;</li> <li>– функции управления информационными ресурсами (файловыми и дисковыми ресурсами), ресурсами печатных служб, службами маршрутизации, удаленного доступа, резервного копирования, службой</li> </ul>

		<p>использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей; составление отчетов по результатам проверок.</p>	<p>терминалов; – эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы.</p> <p>Уметь:</p> <ul style="list-style-type: none"><li>– решать задачу управления безопасностью компьютерных систем;</li><li>– применять инструментальные средства проведения мониторинга защищенности компьютерных систем;</li><li>– применять методы анализа защищенности компьютерных систем и сетей;</li><li>– структурировать аналитическую информацию для включения в отчет;</li><li>– администрировать ресурсы информационной системы в соответствии с реализуемой политикой её безопасности;</li><li>– внедрять списки доступа, позволяющие разрешать или отклонять трафик определенного типа;</li><li>– настраивать фильтрацию трафика с использованием списков контроля доступа;</li><li>– описывать существующую компьютерную сеть, определять требования (влияние используемых приложений, требования пользователей, технические параметры и др.);</li><li>– проводить испытания на прототипе сети WAN и устранять неполадки в корпоративных сетях;</li><li>– проектировать сетевую инфраструктуру в соответствии с потребностями построения информационной системы организации;</li><li>– производить установку и настройку операционных систем серверов и рабочих станций, настраивать сетевое оборудование и сетевые протоколы;</li><li>– работать с протоколом VTP;</li><li>– работать с протоколом связующего дерева STP;</li><li>– разрабатывать и конфигурировать MPLS VPN;</li><li>– разрабатывать технические и коммерческие предложения по созданию и модернизации компьютерной сети для комплекса зданий;</li><li>– создавать каналы в корпоративной сети WAN;</li></ul>
--	--	---	--

			<ul style="list-style-type: none"><li>– создавать локальную сеть в соответствии с утвержденным проектом: настраивать коммутатор с поддержкой технологии VLAN и соединений между коммутаторами.</li></ul> <p>Владеть:</p> <ul style="list-style-type: none"><li>– навыками практической реализации IoT;</li><li>– навыками анализа защищенности компьютерных систем с использованием сканеров безопасности;</li><li>– навыками анализа защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей;</li><li>– навыками составления отчетов по результатам проверок;</li><li>– инструментальными средствами и навыками управления сетевым оборудованием, серверами, устройствами печати, резервного копирования;</li><li>– методами и средствами аудита и мониторинга сетевых устройств и служб;</li><li>– методикой анализа сетевого трафика;</li><li>– навыками анализа требований заказчика и проектирования компьютерной сети;</li><li>– навыками анализа, проектирования и настройки схем потоков трафика в компьютерной сети;</li><li>– навыками мониторинга работы сети, обследования и модернизации сетевого оборудования;</li><li>– навыками настройки коммутации в корпоративной сети;</li><li>– навыками настройки адресации в сети на базе технологий VLSM, NAT и PAT;</li><li>– навыками настройки механизмов фильтрации трафика на базе списков контроля доступа (ACL);</li><li>– навыками настройки протоколов маршрутизации на базе протоколов RIPv2, EIGRP, OSPF;</li><li>– навыками определения влияния приложений на проект сети;</li><li>– навыками оценки качества и соответствия требованиям проекта сети;</li><li>– навыками работы с виртуальными сетями VLAN;</li></ul>
--	--	--	---

				<ul style="list-style-type: none"> <li>– навыками создания и настройки каналов корпоративной сети на базе технологий PPP, PAP, CHAP и Frame Relay;</li> <li>– навыками устранения проблем коммутации, связи, маршрутизации и конфигурации WAN;</li> <li>– навыками фильтрации, контроля и обеспечения безопасности сетевого трафика;</li> <li>– технологиями и навыками построения и администрирования службы каталогов информационной системы организации.</li> </ul>
		<p>ПК-3. Способен проводить анализ безопасности компьютерных систем</p>	<p>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.</p> <p>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.</p> <p>ПК-3.3. Имеет практический опыт (навыки): выполнение анализа уязвимости компьютерных систем.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– базовые программные алгоритмы и структуры данных.</li> <li>– роль эллиптических кривых в современных асимметричных шифрах;</li> <li>– формальные требования, предъявляемые к криптографическим эллиптическим кривым;</li> <li>– методы проникновения в компьютерные системы, используемые современным вредоносным программным обеспечением;</li> <li>– методы функционирования современного вредоносного программного обеспечения.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– применять базовые алгоритмы и структуры данных при решении прикладных задач.</li> <li>– анализировать криптографические эллиптические кривые на предмет их защищённости;</li> <li>– конструировать эллиптические кривые, обладающие заданными свойствами;</li> <li>– реализовывать современные атаки на компьютерные системы;</li> <li>– исследовать вредоносное программное обеспечение.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками реализации базовых алгоритмов.</li> <li>– навыками разработки и конфигурирования программно-аппаратных средств криптографической защиты информации, основанных на криптографических эллиптических кривых;</li> </ul>

				<ul style="list-style-type: none"> <li>– инструментами проведения современных атак на компьютерные системы;</li> <li>– навыками использования инструментальных средств исследования вредоносного программного обеспечения.</li> </ul>
		<p>ПК-4. Способен разрабатывать требования и рекомендации к системам защиты информации в web-приложениях</p>	<p>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.</p> <p>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.</p> <p>ПК-4.3. Имеет практический опыт (навыки): использования средств защиты информации; использования нормативные правовые акты в области защиты информации; разработки руководящих документов по защите</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– математические модели безопасности компьютерных систем.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проводить анализ математических моделей безопасности компьютерных систем.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками разработки математических моделей безопасности компьютерных систем.</li> </ul>

			информации.	
		ПК-5. Способен управлять аналитическими работами и подразделениями	<p>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.</p> <p>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.</p> <p>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.</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– информацию об аналитических ресурсах и компетенциях;</li> <li>– информацию об управлении процессами разработки и сопровождения требований к системам и управление качеством систем;</li> <li>– инфраструктуру разработки и сопровождения требований к системе.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– разрабатывать технико-коммерческие предложения;</li> <li>– разрабатывать методики выполнения аналитических работ;</li> <li>– организовывать аналитические работы в ИТ-проекте;</li> <li>– контролировать проведение аналитических работ в ИТ-проекте.</li> </ul> <p>Владеть:</p> <ul style="list-style-type: none"> <li>– навыками планирования аналитических работ в ИТ-проекте;</li> <li>– навыками составления отчетов об аналитических работах в ИТ-проекте;</li> <li>– навыками оценки квалификации сотрудников в ИТ-проекте.</li> </ul>

**ФТД Факультативные дисциплины**

ФТД.01	Технология программирования и работы на ЭВМ	ПК-5: Способен управлять аналитическими работами и подразделениями	<p>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.</p> <p>ПК-5.2. Демонстрирует умения: разрабатывать технико-коммерческого предложения; разрабатывать методики выполнения аналитических работ; организовывать аналитические работы в ИТ-проекте; контролировать</p>	<p>Знать:</p> <ul style="list-style-type: none"> <li>– определения архитектуры ЭВМ; механизмы организации вычислений; принципы взаимодействия структурных элементов ЭВМ;</li> <li>– процесс разработки и сопровождения требований к системам и управление качеством систем;</li> <li>– инфраструктуру разработки и сопровождения требований к системе.</li> </ul> <p>Уметь:</p> <ul style="list-style-type: none"> <li>– проводить сбор, обработку и анализ данных для определения ключевых свойств системы;</li> <li>– разрабатывать методики выполнения аналитических работ;</li> <li>– проводить исследование и анализ вычислительных систем.</li> </ul>
--------	---	--	--	---

			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.	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 процедуры решения задач профессиональной деятельности	ОПК-3.1 Знает свойства основных дискретных структур: линейных рекуррентных последовательностей, графов, конечных автоматов, комбинаторных структур. ОПК-3.2 Умеет решать задачи периодичности и эквивалентности для линейных рекуррентных последовательностей и конечных автоматов. ОПК-3.2 Умеет применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач.	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; – 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	ОПК-10.1 Знает основные типы криптографических методов защиты	Знать: – различия между стеганографией и криптографией;

		<p>тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности</p>	<p>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.</p>	<p>– 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.</p>
--	--	--	--	--

