ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЕГИОНАЛЬНЫЙ ИНСТИТУТ БИЗНЕСА И УПРАВЛЕНИЯ»

Рассмотрено и одобрено на заседании
Ученого совета
Протокол № 25/6 от 21 апреля 2025 г.

УТВЕРЖДЕНО
Проректор по учебно - воспитательной
работе и качеству образования
_____ Ю.И.Паничкин
Личная подпись инициалы, фамилия
«21» апреля 2025 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

(наименование дисциплины (модуля))

Направление подготовки	09.03.03 Прикладная информатика
Направленность подготовки (профиль)	Прикладная информатика в экономике
Уровень программы	**бакалавриат**
Форма обучения	**очная, очно-заочная, заочная**

Рязань 2025 г.

1. Цель и задачи освоения дисциплины

Цель освоения дисциплины	Формирование у студентов компетенций в области информационной безопасности и применения на практике методов и средств защиты информации.
Задачи дисциплины	Формирование умения обеспечить защиту информации и объектов информатизации формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли Формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов Формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия Настройка и обслуживание аппаратно-программных средств защиты информации

2. Место дисциплины в структуре ОПОП

Блок 1 «Дисциплины (модули)»	
Дисциплины и практики, знания и умения по которым необходимы как "входные" при изучении данной дисциплины	Информационно-правовые системы Информационные системы и технологии
Дисциплины, практики, ГИА, для которых изучение данной дисциплины необходимо как предшествующее	Вычислительные системы, сети, телекоммуникации Государственная итоговая аттестация

3. Требования к результатам освоения дисциплины

Компетенции обучающегося, формируемые в результате освоения дисциплины. Степень сформированности компетенций

Индикатор	Название	Планируемые результаты обучения	ФОС
ОПК3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
ОПК-3.1	Знать: : принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности	Студент знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Тест
ОПК-3.2	Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности	Студент умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Выполнение реферата

ОПК-3.3	Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научноисследовательской работе с учетом требований информационной безопасности	Студент владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Контрольная работа

4. Структура и содержание дисциплины

Тематический план дисциплины

№	Название темы	Содержание	Литера-тура	Индикаторы
1.	Основы информационной безопасности.	Основные понятия, термины и определения в области информационной безопасности. Механизмы обеспечения Безопасности. Актив. Критерии информационной безопасности. Информация, виды информации. Контроль доступа. Защищаемые помещения. Классификационная схема понятий в области «Защита информации».	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
2.	Защищаемая информация.	Общедоступная информация. Информация ограниченного доступа. Персональные данные. Категории обрабатываемых персональных данных (ПДн). Государственная тайна. Служебная тайна. Коммерческая тайна.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
3.	Классификация автоматизированных систем.	Автоматизированная система. Информационная система персональных данных (ИСПДн). Государственные информационные системы (ГИС). Информационные системы общего пользования (ИСОП). Режимы обработки данных в АС. Определяющие признаки при классификации АС. Классификация автоматизированных систем	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
4.	Классы защищённости автоматизированных систем.	Уровни защищенности персональных данных. Угрозы безопасности ПДн. Уровни защищенности ИСПДн. Класс защищённости ГИС не составляющей государственную тайну. Степени возможного ущерба от нарушения свойств безопасности информации. Класс защищённости ГИС.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
5.	Угрозы и уязвимости информационной безопасности.	Общая классификация угроз и уязвимостей информационных систем. Структура угроз. Составляющие угрозы.	8.1.1, 8.2.1, 8.1.2, 8.2.2,	ОПК-3.1

		Уязвимость. Факторы, воздействующие на информацию. Объективные внутренние факторы. Объективные внешние факторы. Субъективные внутренние факторы. Субъективные внешние факторы. Обобщенная модель способов овладения конфиденциальной информацией.	8.1.3, 8.2.3	ОПК-3.2 ОПК-3.3
6.	Технические каналы утечки информации.	Технический канал утечки информации. Описание угрозы утечки информации по ТКУИ. Источники угроз утечки информации по ТКУИ. Среда распространения информативного сигнала. Источники (носители) информации. Технические каналы утечки информации при ее передаче по каналам связи. Технические каналы утечки речевой информации. Технические каналы утечки информации обрабатываемой ТСПИ. Технические каналы утечки видовой информации.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
7.	Угрозы несанкционированного доступа к информации.	Угрозы НСД (несанкционированные действия). Угрозы непосредственного доступа. Угрозы удаленного доступа. Варианты описания угроз НСД. Источники угроз НСД. Типы нарушителей. Категории внутренних нарушителей. Источники угроз НСД. Основные группы уязвимостей ИС. Причины возникновения уязвимостей. Классификация уязвимостей программного обеспечения. Уязвимости системного ПО. Уязвимости протоколов сетевого взаимодействия. Классификация угроз по условиям реализации. Характеристика угроз, реализуемых с использованием протоколов межсетевого взаимодействия. Анализ сетевого трафика. Сканирование сети. Угроза выявления пароля. Отказ в обслуживании. DDoS-атаки.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
8.	(НСД) Угрозы программно-математических воздействий и нетрадиционных информационных каналов.	Программно-математическое воздействие. Вредоносные программы. Классификация угроз ПМВ. Классификация вредоносного ПО. Вредоносные программы для осуществление НСД. Спам. Зомби-сеть (ботнет). Фишинг. Нетрадиционные информационные каналы. Стегано-графические методы.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
9.	Правовой уровень обеспечения информационной	Международные и российские стандарты в области информационной безопасности. Нормативно-правовые и руководящие документы	8.1.1, 8.2.1, 8.1.2,	

	безопасности.	ФСТЭКа РФ по защите информации от несанкционированного доступа (НСД) к информационным системам. 149-ФЗ «Об информации, информационных технологиях и о защите информации». 152-ФЗ «О персональных данных». 98-ФЗ «О коммерческой тайне». 63-ФЗ «Об электронной подписи» 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».	8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
10.	Построение базовой модели угроз ФСТЭК.	Модель угроз информационной безопасности по Методике ФСТЭК 2021. Процесс разработки. Инвентаризация компонентов информационной системы. Определение возможных негативных последствий от реализации угроз безопасности информации. Модель нарушителей. Базовые инструментальные средства для анализа рисков и управления рисками. Оценка способов реализации (возникновения) угроз безопасности информации. Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
11.	Основные понятия криптографии.	Место криптографии среди других наук. Классификация методов преобразования информации. Основные понятия и определения. Смежные дисциплины. История криптографии.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
12.	Наивная криптография.	Простейшие шифры. Шифр «скитала». Системы шифрования Энея "Диск Энея". Система шифрования Цезаря. Полибианский квадрат.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.2 ОПК-3.3
13.	Формальная криптография. Модульная арифметика.	Простой и расширенный алгоритм Евклида. Модульная арифметика. Операции в системе вычетов Zn. Аддитивная и мультипликативная инверсии. Алгебраические структуры. Группа. Циклические подгруппы. Циклические группы. Кольцо. Поле. Поля GF(pn). Аффинный шифр. Шифр Плейфера. Шифр Виженера. Шифр Хилла.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
14.	Формальная криптография.	Шифр Плейфера (способ многоалфавитной замены). Шифр Уитстона (подстановки биграмм). Основные требование к криптографическим	8.1.1, 8.2.1, 8.1.2, 8.2.2,	ОПК-3.1

		системам (Огюст Керкгоффс в 1883 г). Роторные криптосистемы. ENIGMA. Криптостойкость «Энигмы».	8.1.3, 8.2.3	ОПК-3.2 ОПК-3.3
15.	Научная криптография. Компьютерная криптография.	Этап научной криптографии. Этап научной криптографии. Компьютерная криптография. Требования к криптосистемам. Общепринятые требования к КС. Основы криптоанализа. Методы криптоанализа. Разновидности криптоанализа шифрованных сообщений. Атаки на шифратор. Основные задачи, решаемые в современных ИТКС с использованием СКЗИ. Классификация криптографических алгоритмов.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
16.	Симметричные шифры.	Блочные криптосистемы. Сеть Фейстеля. Сеть Фейстеля, модификации. Функция F = S-box (подстановка, замена). Функция F = P-box (перестановка). Алгоритмы блочного шифрования. Алгоритм блочного шифрования DES. Тройной DES. Алгоритмы блочного шифрования IDEA. Алгоритмы блочного шифрования AES. ГОСТ 34.13-2018 «Режимы работы блочных шифров». Поточные шифры. Основная проблема симметричного шифрования.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
17.	Методы аутентификации сообщений.	Аутентификация сообщений с помощью шифрования. Аутентификация сообщений без шифрования. Кодом аутентичности сообщения (MAC). Алгоритмы хэширования. Защищенные функции хэширования. Алгоритм MD5. Алгоритмы хэширования SHA. Алгоритмы хэширования HMAC. ГОСТ 34.11-2018 «Функция хэширования».	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
18.	Асимметричные шифры.	Общая схема асимметричного шифрования. Шифрование с открытым ключом. Области применения криптосистем с открытым ключом. Асимметричные криптосистемы - RSA. Асимметричные криптосистемы Эль Гамаля (El Gamal). Схема обмена ключами Диффи - Хеллмана. Криптосистемы на основе эллиптических уравнений. Составные криптографические системы.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3

19.	Алгоритмы цифровой подписи.	Цифровая подпись. Требования к цифровой подписи. Алгоритмы асимметричного шифрования (цифровой подписи). Стандарт цифровой подписи DSS. Алгоритм цифровой подписи ECDSA . ГОСТ 34.10-2018 «Процессы формирования и проверки электронной цифровой подписи». Использование цифровой подписи.	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3
20.	Инфраструктура открытых ключей (ИОК/PKI).	Свойства информации, заверенной цифровой подписью. Понятие инфраструктуры. Public Key Infrastructure (PKI) – инфраструктура открытого ключа. Certificate Authority (CA) – сертификационный центр (центр сертификации, ЦС). Дерево OID. Архитектура PKI. Понятие цифрового сертификата (PKC). Основные компоненты PKI. Сертификат открытого ключа. Удостоверяющий Центр (УЦ). Иерархия УЦ. Сетевая архитектура. Гибридная (мостовая) архитектура. Проверка сертификата. Политики УЦ. Криптографическое ядро. Репозиторий. Система стандартов в области PKI (ИОК).	8.1.1, 8.2.1, 8.1.2, 8.2.2, 8.1.3, 8.2.3	ОПК-3.1 ОПК-3.2 ОПК-3.3

Распределение бюджета времени по видам занятий с учетом формы обучения

Форма обучения: очная, 2 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	3	1	0	2	4
2.	3	1	0	2	4
3.	3	1	0	2	6
4.	4	2	0	2	6
5.	4	2	0	2	6
6.	5	1	0	4	6
7.	6	2	0	4	6
8.	6	2	0	4	6
9.	6	2	0	4	6
10.	6	2	0	4	6
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	48	16	0	30	60

Форма обучения: очная, 3 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
11.	3	1	0	2	2
12.	3	1	0	2	2
13.	3	1	0	2	2
14.	3	1	0	2	2
15.	6	2	0	4	2
16.	6	2	0	4	2
17.	6	2	0	4	2
18.	6	2	0	4	2
19.	6	2	0	4	4
20.	6	2	0	4	4
	Промежуточная аттестация				
	4	0	0	0	32
	Консультации				
	0	0	0	0	0
Итого	52	16	0	32	56

Форма обучения: очно-заочная, 2 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	1	1	0	0	6
2.	4	2	0	2	8
3.	4	2	0	2	6
4.	4	2	0	2	8
5.	1	1	0	0	6
6.	3	1	0	2	6
7.	1	1	0	0	8
8.	4	2	0	2	8
9.	4	2	0	2	8
10.	4	2	0	2	8
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	32	16	0	14	76

Форма обучения: очно-заочная, 3 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
11.	1	1	0	0	4
12.	1	1	0	0	4

13.	6	2	0	4	4
14.	1	1	0	0	4
15.	3	1	0	2	4
16.	4	2	0	2	4
17.	4	2	0	2	4
18.	4	2	0	2	4
19.	4	2	0	2	4
20.	4	2	0	2	4
	Промежуточная аттестация				
	4	0	0	0	32
	Консультации				
	0	0	0	0	0
Итого	36	16	0	16	72

Форма обучения: заочная, 2 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	1	0.5	0	0.5	16
2.	0	0	0	0	0
3.	0	0	0	0	0
4.	0	0	0	0	0
5.	1.5	0.5	0	1	16
6.	1.5	1	0	0.5	16
7.	1.5	0.5	0	1	16
8.	1	0.5	0	0.5	16
9.	0.5	0	0	0.5	14
10.	1	1	0	0	0
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	10	4	0	4	98

Форма обучения: заочная, 3 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
11.	1	1	0	0	6
12.	0	0	0	0	6
13.	2	1	0	1	6
14.	0	0	0	0	6
15.	0	0	0	0	6
16.	2	1	0	1	6

17.	2	0	0	2	6
18.	1	0	0	1	6
19.	2	0	0	2	6
20.	2	1	0	1	6
	Промежуточная аттестация				
	4	0	0	0	32
	Консультации				
	0	0	0	0	0
Итого	16	4	0	8	92

5. Методические указания для обучающихся по освоению дисциплины

В процессе освоения дисциплины обучающемуся необходимо посетить все виды занятий, предусмотренные рабочей программой дисциплины и выполнить контрольные задания, предлагаемые преподавателем для успешного освоения дисциплины. Также следует изучить рабочую программу дисциплины, в которой определены цели и задачи дисциплины, компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения. Рассмотреть содержание тем дисциплины; взаимосвязь тем лекций и практических занятий; бюджет времени по видам занятий; оценочные средства для текущей и промежуточной аттестации; критерии итоговой оценки результатов освоения дисциплины. Ознакомиться с методическими материалами, программно-информационным и материально техническим обеспечением дисциплины.

Работа на лекции

Лекционные занятия включают изложение, обсуждение и разъяснение основных направлений и вопросов изучаемой дисциплины, знание которых необходимо в ходе реализации всех остальных видов занятий и в самостоятельной работе обучающегося. На лекциях обучающиеся получают самые необходимые знания по изучаемой проблеме. Непременным условием для глубокого и прочного усвоения учебного материала является умение обучающихся сосредоточенно слушать лекции, активно, творчески воспринимать излагаемые сведения. Внимательное слушание лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, конспектирование их помогает усвоить материал. Конспект является полезным тогда, когда записано самое существенное, основное. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку. Принципиальные места, определения, формулы следует сопровождать замечаниями. Работая над конспектом лекций, всегда следует использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал лектор.

Практические занятия

Подготовку к практическому занятию следует начинать с ознакомления с лекционным материалом, с изучения плана практических занятий. Определившись с проблемой, следует обратиться к рекомендуемой литературе. Владение понятийным аппаратом изучаемого курса является необходимым, поэтому готовясь к практическим занятиям, обучающемуся следует активно пользоваться справочной литературой: энциклопедиями, словарями и др. В ходе проведения практических занятий, материал, излагаемый на лекциях, закрепляется, расширяется и дополняется при подготовке сообщений, рефератов, выполнении тестовых работ. Степень освоения каждой темы определяется преподавателем в ходе обсуждения ответов обучающихся.

Самостоятельная работа

Обучающийся в процессе обучения должен не только освоить учебную программу, но и приобрести навыки самостоятельной работы. Самостоятельная работа обучающихся играет важную роль в воспитании сознательного отношения самих обучающихся к овладению теоретическими и практическими знаниями, привитии им привычки к направленному интеллектуальному труду. Самостоятельная работа проводится с целью углубления знаний по дисциплине. Материал, законспектированный на лекциях, необходимо регулярно дополнять сведениями из литературных источников, представленных в рабочей программе. Изучение литературы следует начинать с освоения

соответствующих разделов дисциплины в учебниках, затем ознакомиться с монографиями или статьями по той тематике, которую изучает обучающийся, и после этого – с брошюрами и статьями, содержащими материал, дающий углубленное представление о тех или иных аспектах рассматриваемой проблемы. Для расширения знаний по дисциплине обучающемуся необходимо использовать Интернет-ресурсы и специализированные базы данных: проводить поиск в различных системах и использовать материалы сайтов, рекомендованных преподавателем на лекционных занятиях.

Подготовка к сессии

Основными ориентирами при подготовке к промежуточной аттестации по дисциплине являются конспект лекций и перечень рекомендуемой литературы. При подготовке к сессии обучающемуся следует так организовать учебную работу, чтобы перед первым днем начала сессии были сданы и защищены все практические работы. Основное в подготовке к сессии – это повторение всего материала курса, по которому необходимо пройти аттестацию. При подготовке к сессии следует весь объем работы распределять равномерно по дням, отведенным для подготовки, контролировать каждый день выполнения работы.

6. Фонды оценочных средств для текущего контроля успеваемости, промежуточной аттестации и самоконтроля по итогам освоения дисциплины

Технология оценивания компетенций фондами оценочных средств:

- формирование критериев оценивания компетенций;
- ознакомление обучающихся в ЭИОС с критериями оценивания конкретных типов оценочных средств;
- оценивание компетенций студентов с помощью оценочных средств;
- публикация результатов освоения ОПОП в личном кабинете в ЭИОС обучающегося;

Тест для формирования «ОПК-3.1»

Вопрос №1 .

Выберите несколько значений/

Модели реализации доступа субъектов к объектам

Тип ответа: Многие из многих
Варианты ответов:

1. Дискреционный
2. Уполномоченный
3. Мандатный
4. Безвозмездный
5. Ролевой

Вопрос №2 .

Количество грифов секретности сведений и их носителей…

Варианты ответов:

1. 1
2. 2
3. 3
4. 4
5. 5

Вопрос №3 .

«Информационная система» это

Варианты ответов:

1. совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему
2. совокупность информации, технических средств и персонала, обслуживающего информационную

систему
3. совокупность информации, информационных технологий и технических средств
4. совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему
5. совокупность информационных технологий и технических средств

Вопрос №4 .

Выберите несколько значений/

К рекомендуемым методам и способам защиты информации в информационных системах относятся:

Тип ответа: Многие из многих
Варианты ответов:

1. методы и способы защиты информации от утечки по техническим каналам
2. методы и способы сокрытия информации от внутренних нарушителей
3. методы и способы защиты информации от несанкционированного доступа
4. методы и способы устранения конкурентов

Вопрос №5 . К основным видам политики безопасности не относится следующая:

Варианты ответов:

1. дискреционная
2. матричная (двухмерная)
3. трехмерная
4. избирательная

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	от 0% до 30% правильных ответов из общего числа тестовых заданий
Удовлетворительно	от 31% до 50% правильных ответов из общего числа тестовых заданий
Хорошо	от 51% до 80% правильных ответов из общего числа тестовых заданий
Отлично	от 81% до 100% правильных ответов из общего числа тестовых заданий

Выполнение реферата для формирования «ОПК-3.2»

1. Классификация информации. Виды данных и носителей.

2. Ценность информации. Цена информации.

3. Количество и качество информации.

4. Виды защищаемой информации.

5. Демаскирующие признаки объектов защиты.

6. Классификация источников и носителей информации.

7. мероприятия по управлению доступом к информации.

8. Функциональные источники сигналов. Опасный сигнал.

9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.

10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.

11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.

12. Виды угроз безопасности информации.

13. Основные принципы добывания информации.

14. Процедура идентификации, как основа процесса обнаружения объекта.

15. Методы синтеза информации.

16. Методы несанкционированного доступа к информации.

17. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.

18. Способы наблюдения с использованием технических средств.

19. Каналы утечки информации. Технические каналы утечки

20. Классификация технических каналов утечки по физической природе носителя.

21. Классификация технических каналов утечки по информативности.

22. Классификация технических каналов утечки по времени функционирования.

23. Классификация технических каналов утечки по структуре.

24. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.

25. Перехват электромагнитных излучений.

26. Акустическое подслушивание. Эффекты, возникающие при подслушивании.

27. Понятия скрытия информации, виды скрытий. Информационный портрет.

28. Противодействие наблюдению. Способы маскировки.

29. Способы и средства противодействия подслушиванию.

30. Нейтрализация закладных устройств.

31. Состав инженерной защиты и технической охраны объектов.

32. Инженерные конструкции и сооружения для защиты информации. Их классификация.

33. Средства идентификации личности.

34. Классификация датчиков охранной сигнализации.

35. Классификация извещателей.

36. Телевизионные системы наблюдения.

37. Основные средства системы видеоконтроля.

38. Защита личности как носителя информации.

39. Системный подход к защите информации.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области

Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Выполнение реферата для формирования «ОПК-3.2»

Цели и задачи защиты информации.

Проблемы защиты информации.

Этапы развития концепции обеспечения безопасности информации.

Общие теоретические принципы теории безопасности.

Общие методические принципы теории безопасности.

Проблемы информационного противоборства.

Государственная политика в информационной сфере.

Региональные проблемы информационной безопасности.

Современная доктрина информационной безопасности Российской Федерации.

Современная концепция информационной безопасности.

Основное содержание теории защиты информации.

Общеметодологические принципы формирования теории защиты информации.

Модели систем и процессов защиты информации.

Особенности и состав научно-методологического базиса решения задач защиты информации.

Нечеткие множества.

Нестрогая математика.

Методы оценки.

Неформальный поиск оптимальных решений.

Требования системного подхода к защите информации.

Условия обеспечения требований безопасности. Виды обеспечения системы информационной безопасности.

Концептуальная модель информационной безопасности.

Критерии, условия и принципы отнесения информации к защищаемой.

Количественная и качественная оценки ценности информации. Категории важности информации.

Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности: государственная тайна, коммерческая тайна, коммерческая информация, персональная информация, информация для внутреннего пользования и др.

Виды и типы угроз безопасности.

Классификацияугроз.

Классификация угроз конфиденциальности, целостности и доступности информации.

Изменение активности угроз в зависимости от стадии жизненного цикла.

Формирование и коррекция кортесов

потенциальных угроз.

Источники, виды и методы дестабилизирующего во

здействия на защищаемую информацию.

Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.

Виды уязвимости информации и формы ее проявления.

Каналы несанкционированного получения информации.

Радиоканалы утечки информации.

Акустические каналы утечки информации.

Электрические каналы утечки информации.

Визуально-оптические каналы утечки информации.

Материально-вещественные каналы утечки информации.

Линии связи.

Каналы утечки информации при эксплуатации ЭВМ.

Методы и средства несанкционированного получения информации по техническим каналам.

Методы и средства разрушения информации.

Направления, виды и особенности деятельности спецслужб по несанкционированному доступу к конфиденциальной информации.

Система мер, направленных на обеспечение информационной безопасности.

Подходы к созданию комплексной системы защиты информации.

Виды защиты информации. Характеристики защитных действий.

Кадровое и ресурсное обеспечение защиты информации.

Современные методы и средства оценивания состояния безопасности информационных систем: препятствие, управление доступом, маскировка, регламентация, принуждение, побуждение.

Классификация средств защиты информации.

Технические средства защиты информации.

Программные средства защиты.

Программно-технические средства защиты.

Криптографическая защита.

Скремблирование.

Стеганография.

Законодательные средства.

Организационные средства защиты.

Морально-этические средства.

Кадровое и ресурсное обеспечение защиты информации.

Построение систем защиты информации.

Определение и общеметодологические принципы построения систем защиты информации.

Основы архитектурного построения систем защиты.

Функциональное, организационное и структурное построение систем защиты информации.

Типизация систем защиты.

Стандартизация систем защиты. Современные факторы, влияющие на защиту информации

Критерии оценки выполнения задания

Оценка	Критерии оценивания

Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Выполнение реферата для формирования «ОПК-3.2»

1. Понятие информационной безопасности. Информационная безопасность личности, общества и государства. Конфиденциальная информация.
2. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
3. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
4. Общая характеристика угроз доступности.
5. Общая характеристика угроз целостности.
6. Общая характеристика угроз конфиденциальности.
7. Обобщенные модели системы защиты информации в КС. Одноуровневые и многоуровневые модели. Общая характеристика средств и методов защиты информации в КС.
8. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
9. Отечественное законодательство в области информации и защиты информации.
10. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями. Дублирование информации. Технология RAID. Резервирование технических средств.
11. Общая характеристика технических каналов утечки информации в КС.
12. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
13. Средства и методы разграничения доступа к ресурсам КС.
14. Защита программных средств КС от несанкционированного копирования и исследования.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Выполнение реферата для формирования «ОПК-3.2»

1. Методы борьбы с фишинговыми атаками.
2. Законодательство о персональных данных.
3. Защита авторских прав.
4. Назначение, функции и типы систем видеозащиты.
5. Как подписывать с помощью ЭЦП электронные документы различных форматов.
6. Обзор угроз и технологий защиты Wi-Fi-сетей.
7. Проблемы внедрения дискового шифрования.
8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
9. Особенности процессов аутентификации в корпоративной среде.
10. Квантовая криптография.
11. Утечки информации: как избежать. Безопасность смартфонов.
12. Безопасность применения пластиковых карт - законодательство и практика.
13. Защита CD- и DVD-дисковот копирования.
14. Современные угрозы и защита электронной почты.
15. Программные средства анализа локальных сетей на предмет уязвимостей.
16. Безопасность применения платежных систем - законодательство и практика.
17. Аудит программного кода по требованиям безопасности.
18. Антишпионское ПО (antispyware).
19. Обеспечение безопасности Web-сервисов.
20. Защита от внутренних угроз.
21. Технологии RFID.
22. Уничтожение информации на магнитных носителях.
23. Ботнеты - плацдарм современных кибератак.
24. Цифровые водяные знаки в изображениях.
25. Электронный документооборот. Модели нарушителя.
26. Идентификация по голосу. Скрытые возможности.
27. Безопасность океанских портов.
28. Безопасность связи.
29. Безопасность розничной торговли.
30. Банковская безопасность.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Контрольная работа для формирования «ОПК-3.3»

На основе анализа определений различных понятий, относящихся к данной предметной области, сформулировать определение понятия «чрезвычайная ситуация» в отношении процессов защиты информации;

Определить критерии, по которым можно провести классификацию потенциально возможных чрезвычайных ситуаций, способных влиять на функционирование комплексной системы защиты информацмм;

Изучить предлагаемую статью, посвященную вопросам разработки программы действий в чрезвычайных ситуациях на примере банка, и самостоятельно сформировать:

а) структуру паспорта риска объекта;

б) структуру группы (комитета) по управлению в условиях ЧС и ликвидации их последствий.

Перечень определений различных понятий, относящихся к категории экстремальных (чрезвычайных) событий:

Авария — опасное происшествие на хозяйствующем субъекте, транспорте или на линиях связи, представляющее угрозу жизни и здоровью людей либо приводящее к разрушению производственных помещений, повреждению или уничтожению оборудования, механизмов, транспортных средств, сырья и готовой продукции, а также к нарушению производственного процесса.

Катастрофа — внезапное бедствие, событие, влекущее за собой тяжелые последствия.

Кризисная ситуация — резкий, крутой перелом в чем-либо, тяжелое переходное состояние.

Риск — тип реализации опасностей определенного класса, который может быть определен как частота или как вероятность возникновения одного события при наступлении другого события.

Чрезвычайная ситуация — комплекс событий, протекание и результат наступления которых приводит к реализации в районе чрезвычайной ситуации, опасной для жизни и здоровья людей, а также материальных ценностей, нарушение экономической деятельности, нормального жизнеобеспечения, функционирования схем управления и связи, а также экологического равновесия.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не знает большей части основного содержания выносимых на контрольную работу вопросов дисциплины, допускает грубые ошибки в формулировках основных понятий и не умеет использовать полученные знания при решении типовых практических задач
Удовлетворительно	Обучающийся показывает фрагментарный, разрозненный характер знаний, недостаточно правильно формулирует базовые понятия, допускает ошибки в решении практических задач, при этом владеет основными понятиями тем, выносимых на контрольную работу, необходимыми для дальнейшего обучения
Хорошо	Обучающийся твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя
Отлично	Обучающийся показывает всесторонние, систематизированные, глубокие знания вопросов контрольной работы и умение уверенно применять их на практике при решении конкретных задач

Контрольная работа для формирования «ОПК-3.3»

Построить вербальную модель объекта защиты для помещения, где ведутся конфиденциальные переговоры. Описать объект защиты, возможные виброакустические каналы утечки информации, модель поведения внешнего нарушителя, методы, способы и технические средства съема информации, методы, способы и технические решения по защите информации от её утечки по виброакустическому каналу утечки информации.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не знает большей части основного содержания выносимых на контрольную работу вопросов дисциплины, допускает грубые ошибки в формулировках основных понятий и не умеет использовать полученные знания при решении типовых практических задач
Удовлетворительно	Обучающийся показывает фрагментарный, разрозненный характер знаний, недостаточно правильно формулирует базовые понятия, допускает ошибки в решении практических задач, при этом владеет основными понятиями тем, выносимых на контрольную работу, необходимыми для дальнейшего обучения
Хорошо	Обучающийся твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя
Отлично	Обучающийся показывает всесторонние, систематизированные, глубокие знания вопросов контрольной работы и умение уверенно применять их на практике при решении конкретных задач

Контрольная работа для формирования «ОПК-3.3»

Сформулируйте требования, которым должен соответствовать кандидат на должность начальника службы безопасности коммерческой фирмы. Требования необходимо структурировать по критериям:

образование;

интеллектуальные факторы;

личностные факторы;

физические характеристики;

характер.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не знает большей части основного содержания выносимых на контрольную работу вопросов дисциплины, допускает грубые ошибки в формулировках основных понятий и не умеет использовать полученные знания при решении типовых практических задач
Удовлетворительно	Обучающийся показывает фрагментарный, разрозненный характер знаний, недостаточно правильно формулирует базовые понятия, допускает ошибки в решении практических задач, при этом владеет основными понятиями тем, выносимых на контрольную работу, необходимыми для дальнейшего обучения
Хорошо	Обучающийся твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя
Отлично	Обучающийся показывает всесторонние, систематизированные, глубокие знания вопросов контрольной работы и умение уверенно применять их на практике при решении конкретных задач

Контрольная работа для формирования «ОПК-3.3»

Произвести расчёт вероятности защиты и экономического риска физической защиты компьютерного класса.

Исходные данные: Стоимость предмета защиты _____300_____тыс. руб.

Перечень установленных датчиков защиты: _____ИО – 102_____, _____Стекло –3___, _____, _____, Целесообразно ли установка дополнительного датчика и какого ?

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не знает большей части основного содержания выносимых на контрольную работу вопросов дисциплины, допускает грубые ошибки в формулировках основных понятий и не умеет использовать полученные знания при решении типовых практических задач
Удовлетворительно	Обучающийся показывает фрагментарный, разрозненный характер знаний, недостаточно правильно формулирует базовые понятия, допускает ошибки в решении практических задач, при этом владеет основными понятиями тем, выносимых на контрольную работу, необходимыми для дальнейшего обучения
Хорошо	Обучающийся твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя
Отлично	Обучающийся показывает всесторонние, систематизированные, глубокие знания вопросов контрольной работы и умение уверенно применять их на практике при решении конкретных задач

Контрольная работа для формирования «ОПК-3.3»

Построить вербальную модель объекта защиты для помещения, где производится обработка конфиденциальной информации с использованием СВТ (АС). Описать объект защиты, возможные каналы утечки информации, модель поведения инсайдера, методы, способы и технические средства съема информации по системе электропитания и заземления, методы, способы и технические решения по защите информации от её утечки по системе электропитанмя и заземления.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не знает большей части основного содержания выносимых на контрольную работу вопросов дисциплины, допускает грубые ошибки в формулировках основных понятий и не умеет использовать полученные знания при решении типовых практических задач
Удовлетворительно	Обучающийся показывает фрагментарный, разрозненный характер знаний, недостаточно правильно формулирует базовые понятия, допускает ошибки в решении практических задач, при этом владеет основными понятиями тем, выносимых на контрольную работу, необходимыми для дальнейшего обучения
Хорошо	Обучающийся твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя
Отлично	Обучающийся показывает всесторонние, систематизированные, глубокие знания вопросов контрольной работы и умение уверенно применять их на практике при решении конкретных задач

Вопросы для проведения промежуточной аттестации по итогам освоения дисциплины

Тема 1. Основы информационной безопасности.

1. Механизмы обеспечения Безопасности.
2. Актив.
3. Конфиденциальность информации.
4. Целостность информации
5. Доступность информации.
6. Контроль доступа.
7. Защищаемые помещения.
8. Классификационная схема понятий в области «Защита информации».

Тема 2. Защищаемая информация.

9. Общедоступная информация.
10. Информация ограниченного доступа.
11. Персональные данные.
12. Категории обрабатываемых персональных данных (ПДн).
13. Государственная тайна.
14. Служебная тайна.
15. Коммерческая тайна.

Тема 3. Классификация автоматизированных систем.

16. Автоматизированная система.
17. Информационная система персональных данных (ИСПДн).
18. Государственные информационные системы (ГИС).
19. Информационные системы общего пользования (ИСОП).
20. Режимы обработки данных в АС.
21. Определяющие признаки при классификации АС.

22. Классификация автоматизированных систем

Тема 4. Классы защищённости автоматизированных систем.

23. Уровни защищенности персональных данных.
24. Угрозы безопасности ПДн.
25. Уровни защищенности ИСПДн.
26. Класс защищённости ГИС не составляющей государственную тайну.
27. Степени возможного ущерба от нарушения свойств безопасности информации.
28. Класс защищённости ГИС.

Тема 5. Угрозы и уязвимости информационной безопасности.

29. Классификация угроз.
30. Структура угроз.
31. Составляющие угрозы.
32. Уязвимость.
33. Факторы, воздействующие на информацию.
34. Объективные внутренние факторы.
35. Объективные внешние факторы.
36. Субъективные внутренние факторы.
37. Субъективные внешние факторы.
38. Обобщенная модель способов овладения конфиденциальной информацией.

Тема 6. Технические каналы утечки информации.

39. Технический канал утечки информации.
40. Описание угрозы утечки информации по ТКУИ.
41. Источники угроз утечки информации по ТКУИ.
42. Среда распространения информативного сигнала.
43. Источники (носители) информации.
44. Технические каналы утечки информации при ее передаче по каналам связи.
45. Технические каналы утечки речевой информации.
46. Технические каналы утечки информации обрабатываемой ТСПИ.
47. Технические каналы утечки видовой информации

Тема 7. Угрозы несанкционированного доступа к информации.

48. Угрозы НСД (несанкционированные действия).
49. Угрозы непосредственного доступа.
50. Угрозы удаленного доступа.
51. Варианты описания угроз НСД.
52. Источники угроз НСД.
53. Типы нарушителей (внешние)
54. Типы нарушителей (внутренние). Категории внутренних нарушителей.
55. Основные группы уязвимостей ИС.
56. Причины возникновения уязвимостей.
57. Классификация уязвимостей программного обеспечения.
58. Уязвимости системного ПО.
59. Уязвимости протоколов сетевого взаимодействия.
60. Классификация угроз по условиям реализации.
61. Характеристика угроз, реализуемых с использованием протоколов межсетевого взаимодействия.
62. Анализ сетевого трафика.
63. Сканирование сети.
64. Угроза выявления пароля.
65. Отказ в обслуживании. DDoS-атаки.

Тема 8. (НСД) Угрозы программно- математических воздействий и нетрадиционных информационных каналов.

66. Программно-математическое воздействие.
67. Вредоносные программы.

68. Классификация угроз ПМВ.
69. Классификация вредоносного ПО.
70. Вредоносные программы для осуществление НСД.
71. Спам. Зомби-сеть (ботнет).
72. Фишинг.
73. Нетрадиционные информационные каналы.
74. Стегано- графические методы.

Тема 9. Правовой уровень обеспечения информационной безопасности.

75. 149-ФЗ «Об информации, информационных технологиях и о защите информации». 152-ФЗ «О персональных данных». 98-ФЗ «О коммерческой тайне». 63-ФЗ «Об электронной подписи» 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Тема 10. Построение базовой модели угроз ФСТЭК.

76. Модель угроз информационной безопасности по Методике ФСТЭК 2021.
77. Процесс разработки.
78. Инвентаризация компонентов информационной системы.
79. Определение возможных негативных последствий от реализации угроз безопасности информации.
80. Модель нарушителей.
81. Определение источников угроз безопасности информации и оценка возможностей нарушителей.
82. Оценка способов реализации (возникновения) угроз безопасности информации.
83. Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации.

Тема 11. Основные понятия криптографии.

84. Место криптографии среди других наук.
85. Классификация методов преобразования информации.
86. Понятие шифрования
87. Понятие стеганографии.
88. Понятие криптографического кодирования.
89. Понятие сжатия.
90. Основные понятия и определения.
91. История криптографии

Тема 12. Наивная криптография.

92. Простейшие шифры.
93. Шифр «скитала».
94. Системы шифрования Энея "Диск Энея".
95. Система шифрования Цезаря.
96. Полибианский квадрат.

Тема 13. Формальная криптография. Модульная арифметика.

97. Простой и расширенный алгоритм Евклида.
98. Модульная арифметика.
99. Операции в системе вычетов Zn.
100. Аддитивная и мультипликативная инверсии. Алгебраические структуры.
101. Группа. Циклические подгруппы.
102. Циклические группы.
103. Кольцо.
104. Поле.
105. Поля GF(pn).
106. Аффинный шифр.
107. Шифр Плейфера.
108. Шифр Виженера.
109. Шифр Хилла.

Тема 14. Формальная криптография.

110. Шифр Плейфера (способ многоалфавитной замены).
111. Шифр Уитстона (подстановки биграмм).
112. Основные требование к криптографическим системам (Огюст Керкгоффс в 1883 г).
113. Роторные криптосистемы.
114. ENIGMA. Криптостойкость «Энигмы»

Тема 15. Научная криптография. Компьютерная криптография.

115. Этап научной криптографии.
116. Клода Шеннона «Теория связи в секретных системах».
117. Компьютерная криптография.
118. Требования к криптосистемам.
119. Общепринятые требования к КС.
120. Основы криптоанализа.
121. Методы криптоанализа
122. Статистический криптоанализ.
123. Алгебраический криптоанализ.
124. Дифференциальный (или разностный) криптоанализ
125. Линейный криптоанализ.
126. Разновидности криптоанализа шифрованных сообщений.
127. Атаки на шифратор (пассивные).
128. Атаки на шифратор (активные).
129. Основные задачи, решаемые в современных ИТКС с использованием СКЗИ
130. Классификация криптографических алгоритмов

Тема 16. Симметричные шифры.

131. Блочные криптосистемы.
132. Сеть Фейстеля.
133. Сеть Фейстеля, модификации.
134. Функция F = S-box (подстановка, замена).
135. Функция F = P-box (перестановка).
136. Электронная кодовая книга (ECB) - Режим простой замены.
137. Сцепление блоков шифртекста (CBC)- Режим простой замены с зацеплением.
138. Обратная связь по шифртексту (CFB) -Режим гаммирования с обратной связью.
139. Обратная связь по выходу (OFB) - Режим гаммирования.
140. ГОСТ 34.13-2018 «Режимы работы блочных шифров»
141. Поточные шифры.
142. Основная проблема симметричного шифрования.

Тема 17. Методы аутентификации сообщений.

143. Аутентификация сообщений с помощью шифрования.
144. Аутентификация сообщений без шифрования.
145. Кодом аутентичности сообщения (MAC).
146. Алгоритмы хэширования.
147. Защищенные функции хэширования.
148. Алгоритм MD5. Алгоритмы хэширования SHA.
149. Алгоритмы хэширования HMAC.
150. ГОСТ 34.11-2018 «Функция хэширования».

Тема 18. Асимметричные шифры.

151. Общая схема асимметричного шифрования.
152. Шифрование с открытым ключом.
153. Области применения криптосистем с открытым ключом.
154. Асимметричные криптосистемы - RSA.
155. Асимметричные криптосистемы Эль Гамаля (El Gamal).
156. Схема обмена ключами Диффи - Хеллмана.
157. Криптосистемы на основе эллиптических уравнений. Составные криптографические системы.

Тема 19. Алгоритмы цифровой подписи.

158. Цифровая подпись.
159. Требования к цифровой подписи.
160. Алгоритмы асимметричного шифрования (цифровой подписи).
161. Стандарт цифровой подписи DSS.
162. Алгоритм цифровой подписи ECDSA .
163. ГОСТ 34.10-2018 «Процессы формирования и проверки электронной цифровой подписи».
164. Использование цифровой подписи.

Тема 20. Инфраструктура открытых ключей (ИОК/PKI).

165. Свойства информации, заверенной цифровой подписью.
166. Понятие инфраструктуры.
167. Public Key Infrastructure (PKI) – инфраструктура открытого ключа.
168. Certificate Authority (CA) – сертификационный центр (центр сертификации, ЦС).
169. Дерево OID.
170. Архитектура PKI.
171. Понятие цифрового сертификата (PKC).
172. Основные компоненты PKI.
173. Сертификат открытого ключа.
174. Удостоверяющий Центр (УЦ).
175. Иерархия УЦ. Сетевая архитектура. Гибридная (мостовая) архитектура.
176. Проверка сертификата.
177. Политики УЦ. Криптографическое ядро.
178. Репозиторий.
179. Система стандартов в области PKI (ИОК).

Уровни и критерии итоговой оценки результатов освоения дисциплины

	Критерии оценивания	Итоговая оценка
Уровень1. Недостаточный	Незнание значительной части программного материала, неумение даже с помощью преподавателя сформулировать правильные ответы на задаваемые вопросы, невыполнение практических заданий	Неудовлетворительно/Незачтено
Уровень 2. Базовый	Знание только основного материала, допустимы неточности в ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Удовлетворительно/зачтено
Уровень 3. Повышенный	Твердые знания программного материала, допустимые несущественные неточности при ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Хорошо/зачтено
Уровень 4. Продвинутый	Глубокое освоение программного материала, логически стройное его изложение, умение связать теорию с возможностью ее применения на практике, свободное решение задач и обоснование принятого решения	Отлично/зачтено

7. Ресурсное обеспечение дисциплины

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства	1. Microsoft Windows (лицензионное программное обеспечение) 2. Microsoft Office (лицензионное программное обеспечение) 3. Google Chrome (свободно распространяемое программное обеспечение) 4. Kaspersky Endpoint Security (лицензионное программное обеспечение) 5. AnyLogic (свободно распространяемое программное обеспечение) 6. ArgoUML (свободно распространяемое программное обеспечение) 7. ARIS EXPRESS (свободно распространяемое программное обеспечение) 8. Erwin (свободно распространяемое программное обеспечение) 9. Inkscape (свободно распространяемое программное обеспечение) 10. iTALC (свободно распространяемое программное обеспечение) 11. Maxima (свободно распространяемое программное обеспечение) 12. Microsoft SQL Server Management Studio (лицензионное программное обеспечение) 13. Microsoft Visio (лицензионное программное обеспечение) 14. Microsoft Visual Studio (лицензионное программное обеспечение) 15. MPLAB (свободно распространяемое программное обеспечение) 16. Notepad++ (свободно распространяемое программное обеспечение) 17. Oracle VM VirtualBox (свободно распространяемое программное обеспечение) 18. Paint .NET (свободно распространяемое программное обеспечение) 19. SciLab (свободно распространяемое программное обеспечение) 20. WinAsm (свободно распространяемое программное обеспечение) 21. Консультант+ (лицензионное программное обеспечение отечественного производства) 22. GNS 3 (свободно распространяемое программное обеспечение) 23. Спутник (свободно распространяемое программное обеспечение отечественного производства) 24. Microsoft Project (лицензионное программное обеспечение) 25. «Антиплагиат.ВУЗ» (лицензионное программное обеспечение)
Современные профессиональные базы данных	1. Консультант+ (лицензионное программное обеспечение отечественного производства) 2. http://www.garant.ru (ресурсы открытого доступа)
Информационные справочные системы	1. https://elibrary.ru - Научная электронная библиотека eLIBRARY.RU (ресурсы открытого доступа) 2. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа) 3. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа) 4. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)
Интернет-ресурсы	1. http://window.edu.ru - Информационная система "Единое окно доступа к образовательным ресурсам" 2. https://openedu.ru - «Национальная платформа открытого образования» (ресурсы открытого доступа)

Материально-техническое обеспечение	Учебные аудитории для проведения: занятий лекционного типа, обеспеченные наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации, помещения для хранения и профилактического обслуживания учебного оборудования. Лаборатории и кабинеты: 1. Учебная аудитория Лаборатория информатики Компьютерный класс , включая оборудование: Комплекты учебной мебели, демонстрационное оборудование – проектор и компьютер, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, доска, персональные компьютеры.

8. Учебно-методические материалы

№	Автор	Название	Издательство	Год издания	Вид издания	Кол-во в библио-теке	Адрес электронного ресурса	Вид доступа
1	2	3	4	5	6	7	8	9
8.1 Основная литература								
8.1.1	Сафиуллина Л.Х. Касимова А.Р. Рябов Я.С. Садыков А.М. Богомолов В.А.	Информационная безопасность. Практические аспекты	Интермедия	2021	учебник	-	https://www.iprbookshop.ru/103997.html	по логину и паролю
8.1.2	Басалова Г.В.	Основы криптографии	Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2024	учебное пособие	-	https://www.iprbookshop.ru/133959.html	по логину и паролю
8.1.3	Галатенко В.А.	Основы информационной безопасности	Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2024	учебное пособие	-	https://www.iprbookshop.ru/142285.html	по логину и паролю
8.2 Дополнительная литература								
8.2.1	Ревнивых А.В.	Информационная безопасность в организациях	Ай Пи Ар Медиа	2021	учебное пособие	-	http://www.iprbookshop.ru/108227.html	по логину и паролю
8.2.2	Тесленко И.Б. Виноградов Д.В. Губернаторов А.М. Крылов В.Е. Куликова И.Ю. Муравьева Н.В. Субботина Н.О. Уланов Е.А.	Информационная безопасность	Издательство Владимирского государственного университета	2023	учебное пособие	-	https://www.iprbookshop.ru/143816.html	по логину и паролю
8.2.3	Фороузан Б.А.	Криптография и безопасность сетей	Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2025	учебное пособие	-	https://www.iprbookshop.ru/146352.html	по логину и паролю

9. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья

В РИБиУ созданы специальные условия для получения высшего образования по образовательным программам обучающимися с ограниченными возможностями здоровья (ОВЗ).

Для перемещения инвалидов и лиц с ограниченными возможностями здоровья в РИБиУ созданы специальные условия для беспрепятственного доступа в учебные помещения и другие помещения, а также их пребывания в указанных помещениях с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При получении образования обучающимся с ограниченными возможностями здоровья при необходимости предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература. Также имеется возможность предоставления услуг ассистента, оказывающего обучающимся с ограниченными возможностями здоровья необходимую техническую помощь, в том числе услуг сурдопереводчиков и тифлосурдопереводчиков.

Получение доступного и качественного высшего образования лицами с ограниченными возможностями здоровья обеспечено путем создания в институте комплекса необходимых условий обучения для данной категории обучающихся. Информация о специальных условиях, созданных для обучающихся с ограниченными возможностями здоровья, размещена на сайте университета (https://www.mfua.ru/sveden/objects/#objects).

Для обучения инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата обеспечиваются и совершенствуются материально-технические условия беспрепятственного доступа в учебные помещения, столовую, туалетные, другие помещения, условия их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и др.).

Для адаптации к восприятию обучающимися инвалидами и лицами с ОВЗ с нарушенным слухом справочного, учебного материала, предусмотренного образовательной программой по выбранным направлениям подготовки, обеспечиваются следующие условия:

для лучшей ориентации в аудитории, применяются сигналы, оповещающие о начале и конце занятия (слово «звонок» пишется на доске);
внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
разговаривая с обучающимся, педагог смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих инвалидов и лиц с ОВЗ проводится за счет:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию инвалидами и лицами с ОВЗ с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой РИБиУ по выбранной специальности, обеспечиваются следующие условия:

ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
в начале учебного года обучающиеся несколько раз проводятся по зданию РИБиУ для запоминания месторасположения кабинетов, помещений, которыми они будут пользоваться;
педагог, его собеседники, присутствующие представляются обучающимся, каждый раз называется тот, к кому педагог обращается;
действия, жесты, перемещения педагога коротко и ясно комментируются;
печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;
обеспечивается необходимый уровень освещенности помещений;
предоставляется возможность использовать компьютеры во время занятий и право записи

объяснения на диктофон (по желанию обучающегося).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ определяется преподавателем в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ с учетом его индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.