МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Брянский государственный технический университет» (БГТУ)

Факультет информационных технологий

(наименование факультета/института)

Системы информационной безопасности

(наименование кафедры, ответственной за реализацию дисциплины)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 3E0E6C00DDAD69AC496A79E33A58FAAB
Владелец: Федонин Олег Николаевич
Действителен: с 11.11.2021 до 11.02.2023

УТВЕРЖДАЮ
Первый проректор
по учебной работе и цифровизации
_____ В.А. Шкаберин
«___» _____ 20 __ г.

РАБОЧАЯ ПРОГРАММА

учебной дисциплины

Методы и системы защиты информации, информационная безопасность

(наименование дисциплины)

10.06.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Методы и системы защиты информации, информационная безопасность

(направленность (профиль)/ специализация образовательной программы)

высшее образование – подготовка кадров высшей квалификации

(уровень образования)

Исследователь. Преподаватель-исследователь

(квалификация, присваиваемая по специальности или направлению подготовки)

Очная

(форма обучения)

2020

(год набора)

Брянск 2022

Методы и системы защиты информации, информационная безопасность

(наименование дисциплины)

10.06.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Методы и системы защиты информации, информационная безопасность

(направленность (профиль)/ специализация образовательной программы)

Разработал:

Заведующий кафедрой «СИБ», к.т.н., доцент		М.Ю. Рытов
(должность, ученая степень, ученое звание)	*(подпись)*	*(И.О. Фамилия)*

Рассмотрена и одобрена на заседании кафедры Системы информационной безопасности

(наименование кафедры, ответственной за реализацию дисциплины)

«25» марта 2022 г., протокол № 7

Заведующий кафедрой к.т.н., доцент		М.Ю. Рытов
(ученая степень, ученое звание)	*(подпись)*	*(И.О. Фамилия)*

Предисловие.

Дисциплина «Методы и системы защиты информации, информационная безопасность» направлена на подготовку к сдаче кандидатского экзамена по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

1. Цель освоения дисциплины.

Целью освоения дисциплины является подготовка обучающихся к сдаче кандидатского экзамена по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

2. Место дисциплины в структуре ОПОП.

Дисциплина «Методы и системы защиты информации, информационная безопасность» относится к обязательным дисциплинам вариативной части ОПОП по направлению подготовки 10.06.01 «Информационная безопасность», направленность (профиль) «Методы и системы защиты информации, информационная безопасность».

Дисциплина «Математическое моделирование процессов защиты информации» изучается в 6 семестре.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Таблица 1

Компетенции и требования к освоению дисциплины

Коды компетенций по ФГОС ВО	Наименование компетенции	Результат освоения
Общепрофессиональные компетенции		
ОПК-1	способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	**знать:** методы стимуляции процесса мышления, методы принятия решений, методы оптимизации; **уметь:** распознавать возможности улучшения параметров качества объекта исследования и прогнозировать результат этих улучшений; **владеть:** навыками распознавания возможностей совершенствования методов и средств защиты информации; методами оценки новых технических решений на основе многокритериального подхода;
ОПК-2	способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	**знать:** методологические особенности и принципы построения частных методов исследования; **уметь:** применять разработанные частные методы исследования в научно-исследовательской деятельности в области защиты информации; **владеть:** навыками применения частных методов исследования при решении конкретных задач в области защиты информации;

ОПК-3	способностью обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	**знать:** действующие стандарты в области информационной безопасности; **уметь:** обоснованно выбирать методы оценки степени соответствия защищаемых объектов требованиям действующих стандартов в области информационной безопасности; **владеть:** навыками применения методов оценки степени соответствия защищаемых объектов требованиям действующих стандартов в области информационной безопасности;
ОПК-4	способностью организовать работу коллектива по проведению научных исследований в области информационной безопасности	**знать:** методы и способы организации проведения научных исследований; **уметь:** обоснованно выбирать методы и способы организации проведения научных исследований в области информационной безопасности; **владеть:** навыками применения методов и способы организации проведения научных исследований в области информационной безопасности;
Профессиональные компетенции		
ПК-1	Углубленное изучение теоретических и методологических основ проектирования, эксплуатации и развития систем защиты информации	**знать:** общие направления научных исследований в области развития методов и средств защиты информации и систем на их базе; **уметь:** обоснованно критиковать существующие и вновь создаваемые технические решения; прогнозировать направления развития в области совершенствования методов и средств защиты информации; **владеть:** методиками анализа эффективности технических решений;
ПК-2	Способность ставить и решать инновационные задачи, связанные с разработкой методов и технических средств, повышающих эффективность эксплуатации и проектирования средств защиты информации с использованием глубоких фундаментальных и специальных знаний, аналитических методов и сложных моделей в условиях неопределенности	**знать:** численные методы решения систем уравнений; особенности математического моделирования различных по характеру явлений и процессов существующих и вновь разрабатываемых систем информационной безопасности; методы структурной и параметрической оптимизации; **уметь:** в совершенстве создавать математические модели рабочих процессов и явлений существующих и вновь разрабатываемых систем информационной безопасности; **владеть** навыками математического моделирования рабочих процессов и явлений существующих и вновь разрабатываемых систем информационной безопасности;; навыками анализа результатов математического моделирования рабочих процессов и явлений существующих и вновь разрабатываемых систем информационной безопасности;
ПК-3	Умение проводить анализ, самостоятельно ставить задачу исследования наиболее актуальных проблем, имеющих значение для защиты информации, грамотно планировать эксперимент и осуществлять его на практике	**знать** особенности проведения экспериментальных исследований объектов информационной безопасности; методы планирования натурных и компьютерных экспериментов; методы обработки результатов экспериментальных и компьютерных исследований; **уметь:** планировать технический эксперимент; обрабатывать результаты технического эксперимента; адекватно оценивать результаты технического эксперимента; планировать компьютерный

		эксперимент; обрабатывать результаты компьютерного эксперимента; адекватно оценивать результаты компьютерного эксперимента; **владеть:** навыками организации экспериментальных исследований в области информационной безопасности; навыками организации и проведения компьютерного эксперимента при исследовании процессов защиты информации;
ПК-4	Умение работать с аппаратурой, выполненной на базе микропроцессорной техники и персональных компьютеров для решения практических задач эксплуатации средств защиты информации	**знать:** особенности построения архитектуры средств вычислительной техники и электроники; **уметь:** выстраивать логически упорядоченные алгоритмы программной и аппаратной реализации средств защиты информации; **владеть:** навыками прикладной и программной реализации алгоритмов, реализуемых в процессах защиты информации;
ПК-5	Способность осуществлять педагогическую деятельность, в том числе подготовка специалистов в области систем защиты информации	**знать:** основные формы и методы обучения студентов технических специальностей в области защиты информации, области их рационального применения; **уметь:** учитывать возможности образовательной среды для обеспечения качества образования в области информационной безопасности; **владеть:** формами и методами обучения студентов направлений специальностей в области информационной безопасности;

4. Объем дисциплины и виды учебной работы.

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов).

Вид учебной работы	Всего часов	Семестр
		6
Аудиторные занятия (всего)	12	12
В том числе:	-	-
Лекции (Л)	6	6
Практические занятия (ПЗ)	6	6
Лабораторные работы (ЛР)	-	-
Самостоятельная работа (СРС) (без учета подготовки к экзамену)	60	60
В том числе:	-	-
Курсовой проект	-	-
Подготовка к занятиям	-	-
Самоподготовка	60	60
Экзамен	36	36
Общая трудоемкость: 108 часов; 3 зачетные единицы	108	108

5. Содержание дисциплины.

5.1. Содержание разделов дисциплины (табл. 2).

Таблица 2

Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела (дидактические единицы)
1	**2**	**3**
1	Теория и методология информационной безопасности	Проблемы развития теории и практики обеспечения информационной безопасности. Терминология, определяющая научную и предметную основу и характер деятельности по обеспечению информационной безопасности. информационные проблемы современного общества. Составляющие информационной безопасности. национальные интересы РФ в информационной сфере. Проблемы и перспективы международного сотрудничества в области ИБ. Понятие и сущность защиты информации. Цели защиты информации. Концептуальная модель информационной безопасности. Предмет защиты информации. информация как объект права собственности. Объект защиты информации. Случайные угрозы. Преднамеренные угрозы. Модель гипотетического нарушителя информационной безопасности. Основные принципы построения системы защиты. методы защиты информации. Минимизация ущерба, дублирование, повышение надежности. Создание отказоустойчивых информационных систем. Оптимизация взаимодействия. Методы и средства ЗИ от традиционного шпионажа и диверсий. Методы и средства защиты от ПЭМИН. Защита от НСД. Модели защиты информации. Криптографические методы ЗИ.
2	Математическое моделирование процессов защиты информации	Определения математической модели и математического моделирования. Требования, предъявляемые к математическим моделям. Области применения математических моделей. Классификация математических моделей по типам, свойствам и назначению. Методы моделирования сложных систем. Общие принципы и средства построения математических моделей процессов защиты информации. Способы построения детерминированных математических моделей. Аналитические и численные методы решения уравнений. Визуализация результатов моделирования. Построение математических моделей на основе экспериментальных данных. Применение корреляционного, регрессионного и дисперсионного анализов. Условия применимости статистического анализа. Оценка достоверности и точности математических моделей.
3	Организационно-правовая защита информации	Обзор нормативно-правовой базы РФ в области обеспечения информационной базы. Общая характеристика организационных методов защиты информации. Требования к построению систем безопасности предприятия. Концептуальная модель информационной безопасности. Виды объектов защиты. Классификация угроз информационной безопасности и виды каналов утечки информации на предприятии. Основные направления организационной защиты информации на предприятии. Характеристика защитных действий. разглашение защищаемой информации. Способы пресечения разглашения защищаемой информации. Противодействие несанкциониро-

		ванному доступу к информации. Государственная тайна и порядок отнесения к ней информации. Защита государственной тайны. Организация режима секретности, его особенности и содержание. Коммерческая тайна и порядок её определения. Организация работ с информацией, составляющей коммерческую тайну. Организация и обеспечение защиты коммерческой тайны на предприятии. Организация инженерно-технической безопасности. Организация безопасности функционирования информационных систем. Проведение аналитико-разведывательной работы. Организационная структура службы безопасности. Организация внутриобъектового режима на предприятия. Организация охраны объектов предприятия. Организация и обеспечение защиты коммерческой тайны на предприятии. Организация инженерно-технической безопасности. Организация безопасности функционирования информационных систем. Проведение аналитико-разведывательной работы. Цели и задачи информационно-аналитической работы. Направления и методы аналитической работы. Этапы выполнения информационно-аналитических исследований производственных ситуаций. Методы выполнения аналитических исследований. Основы конкурентной разведки. Подбор и подготовка кадров. Проверка персонала на благонадежность. Заключение контрактов и соглашений о секретности. Особенности увольнения сотрудников, владеющих конфиденциальной информацией. Подбор и подготовка кадров. Проверка персонала на благонадежность. Заключение контрактов и соглашений о секретности. Особенности увольнения сотрудников, владеющих конфиденциальной информацией. Правовая основа системы лицензирования и сертификации в РФ. Лицензирование деятельности по защите информации. Сертификация средств защиты информации.
4	Инженерно-техническая защита информации	Виды угроз безопасности информации, защищаемой техническими средствами. Принципы добывания и обработки информации техническими средствами. Органы добывания информации. Принципы ведения разведки. Технология добывания информации. Способы доступа к конфиденциальной информации. Добывание информации без физического проникновения в контролируемую зону. Доступ к источникам информации без нарушения государственной границы. Показатели эффективности разведки. Особенности утечки информации по техническим каналам. Характеристики технических каналов утечки информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Акустические каналы утечки информации. Материально-вещественные каналы утечки информации. Комплексное использование каналов утечки информации. Основные способы и принципы работы средств наблюдения объектов, подслушивания и перехвата сигналов. Способы и средства наблюдения: способы и средства наблюдения в оптическом диапазоне, способы и средства наблюдения в радиодиапазоне. Способы и средства перехвата сигналов. Способы и средства подслушивания. Способы и средства добывания информации о радиоактивных веществах. Виды и природа каналов утечки информации при эксплуатации ЭВМ. Анализ возможности утечки информации через ПЭМИ. Спо-

		собы обеспечения ЗИ от утечки через ПЭМИН опасных сигналов акустоэлектрических преобразователей; экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Принципы защиты информации. Основные методы защиты информации техническими средствами. способы и принципы работы средств защиты информации от наблюдения, подслушивания и перехвата. Способы и средства противодействия наблюдению. Способы и средства противодействия подслушиванию. Способы и средства предотвращения записи речи на диктофон. Способы и средства предотвращения записи речи через закладные устройства. Защита информации в каналах связи. Разработка инженерно-технической системы защиты информации объекта. Системный подход к инженерно-технической защите информации. Основные этапы проектирования системы защиты информации техническими средствам. Принципы моделирования объектов защиты и технических каналов утечки информации. Рекомендации по выбору методов и средств инженерно-технической защиты информации. Способы оценки угроз безопасности информации и расходов на техническую защиту. САПР систем инженерно-технической защиты информации. Задачи и место инженерно-технической охраны в системе обеспечения информационной безопасности. Структура системы инженерной защиты и технической охраны объектов. Средства инженерной защиты. Роль и место технических средств в организации режима охраны. Современная концепция защиты объектов. Основные составляющие систем ТСО: датчики, приборы визуального наблюдения, системы сбора и обработки информации, средства связи, питания и тревожно-вызывной сигнализации. Практическая реализация систем ТСО: охрана режимных помещений, проект охраны объектов. Современные систем видеонаблюдения: структура и функции. Нормативно-правовая база инженерно-технической защиты информации. Организационные и технические меры инженерно-технической защиты информации в государственных и коммерческих структурах. Лицензирование деятельности и сертификация средств защиты информации. Аттестация объектов информатизации. Контроль эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Методы расчета и инструментального контроля показателей защиты информации.

5	Программно-аппаратная защита информации	Основные понятия: объект защиты информации, компьютерная система, безопасность информации в КС, система защиты информации. Уязвимость компьютерных систем. Искусственные и естественные угрозы. Каналы утечки информации. Политика безопасности в компьютерных системах. Избирательная политика безопасности. Управление информационными потоками. Оценка защищенности. механизмы защиты. Система документов России. Основные понятия и концепции. Идентификация и аутентификация пользователя. Типовые схемы идентификации и аутентификации пользователя. Особенности применения пароля для аутентификации пользователя. Биометрическая идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Параллельная схема идентификации с нулевой передачей знаний. Схема идентификации гиллоу-куискуотера. Защита информации в КС от несанкционированного доступа. Система разграничения доступа к информации в КС. Управление доступом. Состав системы разграничения доступа. Концепция построения систем разграничения доступа. Организация доступа к ресурсам КС. Обеспечение целостности информации в КС. Полностью контролируемые компьютерные системы. Программная реализация функций КС. Аппаратная реализация функций КС. Частично контролируемые компьютерные системы. Основные элементы и средства защиты от несанкционированного доступа. Защита информации в ПЭВМ. Категории средств защиты информации. Защита информации, обрабатываемой ПЭВМ и ЛВС, от утечки по сети электропитания. Виды мероприятий по защите информации. Современные системы защиты ПЭВМ от несанкционированного доступа к информации. Методы, затрудняющие считывание скопированной информации. Методы, препятствующие использованию скопированной информации. Основные функции средств защиты от копирования. Основные методы защиты от копирования. Классификация средств исследования программ. Методы защиты программ от исследования. Анализ программ на этапе их эксплуатации. Общая характеристика и классификация компьютерных вирусов. Общая характеристика средств нейтрализации компьютерных вирусов. Классификация методов защиты от компьютерных вирусов.
6	Криптографическая защита информации	Алгебраические модели шифров. Модель Шеннона. Понятие шифрвеличины и шифробозначения. Опорный шифр. Детерминированные и стохастические генераторы ключевого потока. Вероятностные модели шифров. Шифры с ограниченным и неограниченным ключом. Открытые сообщения. Алфавиты сообщений. Частотные характеристики сообщений. Избыточность. Математические модели открытых текстов. Критерии распознавания. Цепи Маркова. Энтропия и избыточность языка. Расстояние единственности. Стойкость шифров. Теоретическая стойкость шифров. Практическая стойкость шифров. Теоретико-информационный подход к оценке криптостойкости шифров. Надежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вы-

		числительно стойкие шифры. Рабочая характеристика шифра. Сложность взлома. Аппаратные и термодинамические ограничения. Китайская лотерея. Эквивалентная устойчивость к лобовому вскрытию симметричных и ассиметричных ключей. Принципы рассеивания и перемешивания. Имитостойкость шифров. Имитация и подмена сообщения. Способы обеспечения имитостойкости. Коды аутентификации. Помехостойкость шифров. Шифры, не распространяющие искажений типа "замена знаков". Шифры, не распространяющие искажений типа "пропуск-вставка знаков". Практические вопросы повышения надежности. Принципы построения блочных шифров. Применяемые математические преобразования (операции). Лавинный эффект, диффузия и конфузия. Сеть Файстеля. Матричные преобразования. Современные блочные криптоалгоритмы. Размер блока, размер ключа, количество раундов. Режимы использования блочных шифров. Принципы построения поточных шифрсистем. Управляющие и шифрующие блоки. Генераторы ключевого потока. Истинно случайные и псевдослучайные последовательности. Синхронизация поточныхшифрсистем. Регистры сдвига с обратной связью. Алгоритм Берленкемпа-Месси. Усложнение линейных рекуррентных последовательностей. Примеры поточных шифрсистем. Теоремы об однонаправленной функции и однонаправленной функции с лазейкой. Шифрсистема RSA. Вопросы практической реализации RSA. Взаимосвязь компонентов RSA. Шифрсистема Эль-Гамаля. Вопросы практической реализации шифрсистемы Эль-Гамаля. Шифрсистемы на основе помехоисправляющих кодов Шифрсистема Мак-Элиса. Шифрсистемы на основе маскировки задач полиномиальной сложности. Рюкзачные шифрсистемы. Требования к криптографическим хэш-функциям. Блочно-итерационные и шаговые функции. Ключевые хэш-функции, коды аутентичности сообщений. Бесключевые хэш-функции, коды обнаружения ошибок. Схемы применения ключевых и бесключевых хэш-функций. Современные алгоритмы хеширования. Сравнение свойств собственноручной и цифровой подписи. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата - Шамира. Цифровая подпись Эль-Гамаля. Одноразовые цифровые подписи. Современные алгоритмы цифровой подписи. Протоколы распределения ключей. Передача ключей с использованием симметричного шифрования. Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей. Предварительное распределение ключей. Способы установления ключей для конференц-связи. Схемы разделения секрета. Доказательства с нулевым разглашением. Подбрасывание монеты по телефону. Электронные деньги. Абонентское и канальное шифрование. Области применения программных и аппаратных средств криптозащиты. Аппаратные шифраторы. Смарт-карты. Программные реализации. Выбор средств программной реализации. Типы данных. Хранение ключевой и промежуточной информации. Защита от атак хронометрированием в ассиметричных системах. Режимы шифрования применительно к задачам шифрования. Прозрачное шифрование. Обеспечение помехоустойчивости и имитостойкости. Создание виртуальных

		защищенных дисков.
7	Защита персональных данных	Основные нормативно-правовые акты в области защиты персональных данных. Требования ФЗ «О персональных данных». Понятийный аппарат. Обеспечение конфиденциальности персональных данных. Специальные категории персональных данных. Право субъекта персональных данных на доступ к своим персональным данным. Принципы обработки и хранения персональных данных. Условия обработки персональных данных: согласие субъекта на обработку, обрабатываемые без уведомления персональных данных. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных. Основные нормативно-правовые акты в области защиты персональных данных за рубежом. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28.01.1981 EST № 108. Федеральные органы, уполномоченные в области обеспечения безопасности персональных данных– регуляторы. Сфера деятельности регуляторов.. Понятие информационной системы персональных данных. Условий создания и использования персональных данных: состав персональных данных и цель их обработки; технология обработки; субъекты, создающие и потребляющие персональных данных; правила доступа; используемые объекты. Формы представления персональных данных: акустическая (речевая) информация; видовая информация; информация в виде сигналов; информация в виде логических структур. Техническая структура информационной системы персональных данных: технические средства, используемые каналы связи, программные средства. Информационные потоки, циркулирующие в информационной системе персональных данных. Граничное телекоммуникационное оборудование и виртуальные локальные сети. Характеристик безопасности персональных данных: конфиденциальность, целостность и доступность. Классификационные признаки уровней защищенности испдН: тип угрозы, количество субъектов ПДн, тип ИС. таблица определения уровней защищенности ИСПДн. Классификация угроз безопасности персональных данных. Анализ и характеристики угроз возможной утечки информации по техническим каналам. Анализ и характеристики угроз несанкционированного доступа к информации в информационной системе персональных данных, включая характеристики источников угроз несанкционированного доступа, характеристики уязвимостей системного и прикладного программного обеспечения, характеристики угроз безопасности персональных данных, реализуемых с использованием протоколов межсетевого взаимодействия и программно-математических воздействий, характеристики не-

		традиционных информационных каналов и результатов несанкционированного или случайного доступа. Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах (автоматизированных рабочих местах, локальных и распределенных информационных системах), не имеющих и имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.
8	Управление интеллектуальной собственностью	Основные принципы авторского и патентного права. Объекты права. Имущественные и личные права. Способы гражданско-правовой защиты. Средства индивидуализации. Охрана нетрадиционных объектов. Защита авторских и смежных прав. Защита промышленной собственности. Защита программ для ЭВМ и баз данных. Защита служебной и коммерческой тайны. Защита рационализаторских предложений. Международная патентная система. Всемирная организация интеллектуальной собственности.

5.2. Разделы дисциплины и виды занятий (в часах) (табл.4).

Таблица 4

Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	С	СРС	ЭКЗ	Всего часов
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	Теория и методология информационной безопасности	2	-	-	-	7	4	13
2	Математическое моделирование процессов защиты информации	2	-	-	-	7	4	13
3	Организационно-правовая защита информации	2	-	-	-	7	4	13
4	Инженерно-техническая защита информации	-	2	-	-	7	4	13
5	Программно-аппаратная защита информации	-	2	-	-	7	4	13
6	Криптографическая защита информации	-	2	-	-	7	4	13
7	Защита персональных данных	-	-	-	-	9	6	15
8	Управление интеллектуальной собственностью	-	-	-	-	9	6	15

6. Лекции, практические занятия, лабораторные работы.

6.1. Лекции (табл. 5).

Таблица 5

Тематика лекций и их трудоемкость

№ п/п	№ раздела дисциплины	Тематика лекций	Трудоемкость (час.)
1	**2**	**3**	**4**
1	1	Теория и методология информационной безопасности	2
2	2	Математическое моделирование процессов защиты информации	2
3	3	Организационно-правовая защита информации	2
Итого			6

6.2. Практические занятия (табл. 6).

Таблица 6

Тематика практических занятий и их трудоемкость

№ п/п	№ раздела дисциплины	Тематика практических занятий	Трудоемкость (час.)
1	**2**	**3**	**4**
1	4	Инженерно-технические методы защита информации	2
2	5	Программно-аппаратные методы защита информации	2
3	6	Криптографические методы защиты информации	2
Итого			6

6.3. Образовательные технологии.

В рамках изучения дисциплины предусмотрены следующие образовательные технологии:

Лекции: проводятся в форме мастер-класса преподавателя; используются опорные конспекты (системы слайдов), доводимые до аудитории с помощью мультимедийного оборудования
Практические занятия: проводятся в форме мастер-класса преподавателя; используется контекстное обучение с привязкой разбираемых примеров к реальным конструкциям и условиям их работы
Самостоятельная работа студентов: при проведении самостоятельной работы обучающиеся имеют доступ в лабораторию вычислительной техники кафедры ПТМиО с выходом в сеть «Интернет», а также к электронно-библиотечной системе университета
Консультации: проводятся в форме дискуссии «учебная группа – преподаватель»
Экзамен: письменный, проводится по билетам;

7. Самостоятельная работа студентов (табл. 7).

Таблица 7

№ п/п	№ раздела дисциплины	Вид самостоятельной работы
1	**2**	**3**
1	1	Работа с литературой;
2	2	Работа с литературой;
3	3	Работа с литературой;
4	4	Работа с литературой;
5	5	Работа с литературой;
6	6	Работа с литературой;
7	7	Работа с литературой;
8	8	Работа с литературой;
9	1-8	Подготовка к экзамену

8. Учебно-методическое и информационное обеспечение дисциплины:

8.1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю):

1. Лагерев, В.В. Советы студентам по рациональной организации учебного труда: учеб. пособ. для вузов / В.В. Лагерев. – Брянск: БИТМ, 1992. – 92 с. [259 экз.].
2. Рабочая программа учебной дисциплины «Методы и системы защиты информации, информационная безопасность» для направления подготовки кадров высшей квалификации 10.06.01 «Информационная безопасность», направленность программы «Методы и системы защиты информации, информационная безопасность». [Электронный ресурс каф. СИБ]

8.2. Перечень основной, дополнительной и справочной учебной литературы, необходимой для освоения дисциплины:

а) основная литература

1) Аверченков В.И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 268 с. — 978-89838-487-6. — Режим доступа: http://www.iprbookshop.ru/6991.html

2) Аверченков В.И. Организационная защита информации [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 184 с. — 978-89838-489-0. — Режим доступа: http://www.iprbookshop.ru/7002.html

3) Аверченков В.И. Служба защиты информации. Организация и управление [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 186 с. — 5-89838-138-4. — Режим доступа: http://www.iprbookshop.ru/7008.html

4) Аверченков В.И. Аудит информационной безопасности органов исполнительной власти [Электронный ресурс] : учебное пособие / В.И. Аверченков [и др.]. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 100 с. — 978-89838-491-3. — Режим доступа: http://www.iprbookshop.ru/6992.html

5) Аверченков В.И. Защита персональных данных в организации [Электронный ресурс] : монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. — Электрон. текстовые данные. — Брянск: Брянский государственный технический университет, 2012. — 124 с. — 5-89838-382-4. — Режим доступа: http://www.iprbookshop.ru/6993.html

6) Заляжных, В.А. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем [Электронный ресурс] : учеб.-метод. пособие / В.А. Заляжных, А.В. Гирик. — Электрон. дан. — Санкт-Петербург : НИУ ИТМО, 2014. — 136 с. — Режим доступа: https://e.lanbook.com/book/71193. — Загл. с экрана.

7) Коваленко Ю.И. Методика защиты информации в организациях [Электронный ресурс] : монография / Ю.И. Коваленко, Г.И. Москвитин, М.М. Тараскин. — Электрон. текстовые данные. — М. : Русайнс, 2016. — 162 с. — 978-5-4365-0887-0. — Режим доступа: http://www.iprbookshop.ru/61625.html

8) Лапина М.А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : лабораторный практикум / М.А. Лапина [и др.]. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 242 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62945.html

9) Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 c. — 978-5-7422-4331-1. — Режим доступа: http://www.iprbookshop.ru/43960.html

10) Свинарев Н.А. Инструментальный контроль и защита информации [Электронный ресурс] : учебное пособие / Н.А. Свинарев [и др.]. — Электрон. текстовые данные. — Воронеж: Воронежский государственный университет инженерных технологий, 2013. — 192 c. — 978-5-00032-018-1. — Режим доступа: http://www.iprbookshop.ru/47422.html

б) дополнительная литература

1) Аверченков, В.И. Автоматизация проектирования комплексных систем защиты информации: монография [Электронный ресурс] : монография / В.И. Аверченков, М.Ю. Рытов, О.М. Голембиовская. — Электрон. дан. — Москва : ФЛИНТА, 2017. — 145 с. — Режим доступа: https://e.lanbook.com/book/92913. — Загл. с экрана.

2) Горев А.И. Обработка и защита информации в компьютерных системах [Электронный ресурс] : учебно-практическое пособие / А.И. Горев, А.А. Симаков. — Электрон. текстовые данные. — Омск: Омская академия МВД России, 2016. — 88 c. — 978-5-88651-642-5. — Режим доступа: http://www.iprbookshop.ru/72856.html

3) Кожуханов Н.М. Правовые основы информационной безопасности [Электронный ресурс] : учебное пособие / Н.М. Кожуханов, Е.С. Недосекова. — Электрон. текстовые данные. — М. : Российская таможенная академия, 2013. — 88 c. — 978-5-9590-0725-6. — Режим доступа: http://www.iprbookshop.ru/69749.html

4) Метелица Н.Т. Вычислительные сети и защита информации [Электронный ресурс] : учебное пособие / Н.Т. Метелица. — Электрон. текстовые данные. — Краснодар: Южный институт менеджмента, 2013. — 48 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/25962.html

5) Санников В.Г. Теория информации и кодирования [Электронный ресурс] : учебное пособие / В.Г. Санников. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 95 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61558.html

6) Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 544 c. — 978-5-4488-0074-0. — Режим доступа: http://www.iprbookshop.ru/63592.html

7) Пашинцев В.П. Нестандартные методы защиты информации [Электронный ресурс] : лабораторный практикум / В.П. Пашинцев, А.В. Ляхов. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 196 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63217.html

8) Петренко В.И. Теоретические основы защиты информации [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 222 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63138.html

9) Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

в) справочная литература

1) ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Госстандарт России.

2) ГОСТ Р 51188-98 Защита информации. ИСПЫТАНИЯ ПРОГРАММНЫХ СРЕДСТВ НА НАЛИЧИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ. Типовое руководство. Госстандарт России.

3) ГОСТ Р ИСО/МЭК ТО 15446-2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности». Госстандарт России.

4) ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации». Госстандарт России.

5) ГОСТ Р ИСО/МЭК 15408-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3. Госстандарт России.

6) ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий». Госстандарт России.

7) ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем». Госстандарт России.

8) ГОСТ Р ИСО/МЭК 27006 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности». Госстандарт России.

9) ГОСТ Р ИСО/МЭК 18028-1 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности». Госстандарт России.

10) ГОСТ Р ИСО/МЭК ТО 24762 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения». Госстандарт России.

11) ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации». Госстандарт России.

12) ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Госстандарт России.

13) ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов. Госстандарт России.

14) ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Госстандарт России.

15) ГОСТ Р 53112-2008 Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний. Госстандарт России.

16) ГОСТ Р 53115-2008 Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства. Госстандарт России.

17) ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Госстандарт России.

18) ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска. Госстандарт России.

19) ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Госстандарт России.

20) ГОСТ Р 51275–99. Защита информации. Объект информатизации. Факторы воздействующие на информатизацию. Общие положения. Госстандарт России.

21) ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Госстандарт России.

22) Доктрина информационной безопасности Российской Федерации. 9.09.2000 г., № Пр.–1895.

8.3. Перечень ресурсов сети «Интернет», необходимых для изучения дисциплины:

- Электронная информационно-образовательная среда (ЭИОС) БГТУ:
- www.tu-bryansk.ru - официальный сайт БГТУ;
- edu.tu-bryansk.ru - система электронной поддержки учебных курсов на базе программного обеспечения Moodle со встроенной подсистемой тестирования;
- mark.lib.tu-bryansk.ru/marcweb2 - электронная библиотечная система БГТУ;
- lib.tu-bryansk.ru - сайт библиотеки БГТУ со ссылками на внешние ЭБС;

9. Материально-техническое обеспечение дисциплины.

Специальные помещения:

- помещение для проведения занятий лекционного типа, групповых и индивидуальных консультаций (ауд. Б.303);
- помещение для текущего контроля и промежуточной аттестации, в том числе итоговой аттестации (ауд. 210);
- помещение для самостоятельной работы, оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации (ауд. 224).

Перечисленные специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Перечень необходимого программного обеспечения:

Операционные системы и офисные пакеты (ОС WINDOWS, Linux, LibreOffice).

10. Методические рекомендации по организации изучения дисциплины.

10.1. Методические рекомендации для преподавателей.

При чтении лекций должна решаться задача доступного изложения всех материалов по данной дисциплине согласно рабочей программе.

Главной задачей каждой лекции и практического занятия является раскрытие тематики и увязка с практическим применением машин в производстве.

При чтении лекций и проведении практических занятий целесообразно использовать опорные конспекты (систему слайдов с наглядными изображениями и тезисами лекций).

10.2. Методические рекомендации для обучающихся.

Подготовку по дисциплине «Методы и системы защиты информации, информационная безопасность» можно разбить на несколько этапов:

- работа с литературой;
- подготовка к экзамену.

При подготовке к экзамену необходимо возникающие вопросы задать преподавателю на консультациях.

11. Фонд оценочных средств

11.1. Этапы формирования компетенций

Этапы формирования компетенций (разделы дисциплины)	Показатель освоения (коды)																										
	ОПК-1			ОПК-2			ОПК-3			ОПК-4			ПК-1			ПК-2			ПК-3			ПК-4			ПК-5		
	Р1	Р2	Р3	Р1	Р2	Р3	Р1	Р2	Р3	Р1	Р2	Р3	Р1	Р2	Р3	Р1	Р2	Р3	Р1	Р2	Р3	Р1	Р2	Р3	Р1	Р2	Р3
Теория и методология информационной безопасности	+	+	+	+	+	+				+	+	+	+	+	+				+	+	+	+	+	+	+	+	+
Математическое моделирование процессов защиты информации			+	+	+	+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Организационно-правовая защита информации			+	+	+	+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Инженерно-техническая защита информации			+	+	+	+	+	+	+			+	+	+	+	+	+	+	+	+		+	+	+	+	+	+
Программно-аппаратная защита информации			+	+	+	+						+	+	+	+				+	+	+				+	+	+
Криптографическая защита информации			+	+	+	+						+	+	+	+				+	+	+				+	+	+
Защита персональных данных			+	+	+	+						+	+	+	+				+	+	+				+	+	+
Управление интеллектуальной собственностью			+	+	+	+						+	+	+	+				+	+	+				+	+	+

11.2. Индексированные показатели и критерии оценивания результатов

Коды компетенций по ФГОС ВО	Наименование компетенции	Показатель освоения	Оценочные средства текущего контроля	Оценочные средства промежуточного контроля
Общепрофессиональные компетенции				
ОПК-1	способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	**Р1 – знает**: методы стимуляции процесса мышления, методы принятия решений, методы оптимизации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р2 – умеет: распознавать возможности улучшения параметров качества объекта исследования и прогнозировать результат этих улучшений;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р3 – владеет: навыками распознавания возможностей совершенствования методов и средств защиты информации; методами оценки новых технических решений на основе многокритериального подхода;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
ОПК-2	способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	**Р1 – знает**: **:** методологические особенности и принципы построения частных методов исследования;		
		Р2 – умеет: применять разработанные частные методы исследования в научно-исследовательской деятельности в области защиты информации;		
		Р3 – владеет: навыками применения частных методов исследования при решении конкретных задач в области защиты информации;		

ОПК-3	способностью обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	**Р1 – знает**: действующие стандарты в области информационной безопасности;		
		Р2 – умеет: обоснованно выбирать методы оценки степени соответствия защищаемых объектов требованиям действующих стандартов в области информационной безопасности;		
		Р3 – владеет: навыками применения методов оценки степени соответствия защищаемых объектов требованиям действующих стандартов в области информационной безопасности;		
ОПК-4	способностью организовать работу коллектива по проведению научных исследований в области информационной безопасности	**Р1 – знает**: методы и способы организации проведения научных исследований;		
		Р2 – умеет: обоснованно выбирать методы и способы организации проведения научных исследований в области информационной безопасности;		
		Р3 – владеет: **:** навыками применения методов и способы организации проведения научных исследований в области информационной безопасности;		
Профессиональные компетенции				
ПК-1	Углубленное изучение теоретических и методологических основ проектирования, эксплуатации и развития систем защиты информации	**Р1 – знает**: общие направления научных исследований в области развития методов и средств защиты информации и систем на их базе;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р2 – умеет: обоснованно критиковать существующие и вновь создаваемые технические решения; прогнозировать направления развития в области совершенствования методов и средств защиты информации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену

		Р3 – владеет: методиками анализа эффективности технических решений;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
ПК-2	Способность ставить и решать инновационные задачи, связанные с разработкой методов и технических средств, повышающих эффективность эксплуатации и проектирования средств защиты информации с использованием глубоких фундаментальных и специальных знаний, аналитических методов и сложных моделей в условиях неопределенности	**Р1 – знает**: численные методы решения систем уравнений; особенности математического моделирования различных по характеру явлений и процессов существующих и вновь разрабатываемых систем информационной безопасности; методы структурной и параметрической оптимизации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р2 – умеет: в совершенстве создавать математические модели рабочих процессов и явлений существующих и вновь разрабатываемых систем информационной безопасности;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р3 – владеет: навыками математического моделирования рабочих процессов и явлений существующих и вновь разрабатываемых систем информационной безопасности;; навыками анализа результатов математического моделирования рабочих процессов и явлений существующих и вновь разрабатываемых систем информационной безопасности;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
ПК-3	Умение проводить анализ, самостоятельно ставить задачу исследования наиболее актуальных проблем, имеющих значение для защиты информации, грамотно планировать эксперимент и осуществлять его на практике	**Р1 – знает**: особенности проведения экспериментальных исследований объектов информационной безопасности; методы планирования натурных и компьютерных экспериментов; методы обработки результатов экспериментальных и компьютерных исследований;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену

		Р2 – умеет: планировать технический эксперимент; обрабатывать результаты технического эксперимента; адекватно оценивать результаты технического эксперимента; планировать компьютерный эксперимент; обрабатывать результаты компьютерного эксперимента; адекватно оценивать результаты компьютерного эксперимента;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р3 – владеет: навыками организации экспериментальных исследований в области информационной безопасности; навыками организации и проведения компьютерного эксперимента при исследовании процессов защиты информации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
ПК-4	Умение работать с аппаратурой, выполненной на базе микропроцессорной техники и персональных компьютеров для решения практических задач эксплуатации средств защиты информации	**Р1 – знает**: особенности построения архитектуры средств вычислительной техники и электроники;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р2 – умеет: выстраивать логически упорядоченные алгоритмы программной и аппаратной реализации средств защиты информации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р3 – владеет: навыками прикладной и программной реализации алгоритмов, реализуемых в процессах защиты информации;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
ПК-5	Способность осуществлять педагогическую деятельность, в том числе подготовка специалистов в области систем защиты информации	**Р1 – знает**: основные формы и методы обучения студентов технических специальностей в области защиты информации, области их рационального применения;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену
		Р2 – умеет: учитывать возможности образовательной среды для обеспечения качества образования в области информационной безопасности;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену

		РЗ – владеет: формами и методами обучения студентов направлений специальностей в области информационной безопасности;	Устный опрос (вопросы к экзамену)	Вопросы к экзамену

11.3. Оценочные средства для промежуточной аттестации

Шкала оценивания

Уровень освоения обучающимся учебного материала определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Показатели и критерии оценивания сформированности компетенций

Оценку «отлично» заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебного материала, умение свободно выполнять задания, предусмотренные учебной программой, изучивший основную и знакомый с дополнительной литературой. Во время экзамена обучающийся должен подробно ответить на три теоретических вопроса билета.

Оценку «хорошо» заслуживает обучающийся, обнаруживший полное знание учебного материала, успешно выполнивший предусмотренные учебной программой задания, изучивший основную литературу. Во время экзамена обучающийся должен подробно ответить хотя бы на два теоретических вопроса билета.

Оценку «удовлетворительно» заслуживает обучающийся, обнаруживший знание основного учебного материала в полном объеме, необходимом для дальнейшей учебы и работы по профессии, выполнивший предусмотренные учебной программой задания, знакомый с основной литературой. Во время экзамена обучающийся должен подробно ответить хотя бы на один теоретический вопрос билета и частично на два других вопроса.

Оценку «неудовлетворительно» заслуживает обучающийся, обнаруживший пробелы в знаниях основного учебного материала, допустивший принципиальные ошибки при выполнении предусмотренных программой заданий. Во время экзамена обучающийся частично отвечает на вопросы.

Процедура промежуточной аттестации – письменный экзамен.

Контрольно-измерительные материалы промежуточной аттестации

Вопросы к экзамену по дисциплине

Раздел «Теория и методология информационной безопасности»

1. Понятие информационной безопасности, основные составляющие информационной безопасности.
2. Источники угроз информационной безопасности РФ и их классификация.
3. Определение защиты информации, безопасности информации
4. Политика безопасности и анализ рисков;
5. Сущность информации как объекта права собственности.
6. Раскройте сущность объекта защиты.

7. Классификация угроз информационной безопасности, основные группы классификации.
8. Модель нарушителя информационной безопасности?
9. Основные принципы построения системы защиты информации.
10. Основные модели защиты информации и их особенности.
11. Сущность методов защиты от случайных уг роз
12. Понятия идентификации и аутентификации, основные виды аутентификации.
13. Повышение надежности и отказоустойчивости информационных систем.
14. Особенность построения защиты от несанкционированного доступа

Раздел «Математическое моделирование процессов защиты информации»

15. Определения математической модели и математического моделирования.
16. Требования, предъявляемые к математическим моделям.
17. Области применения математических моделей.
18. Классификация математических моделей по типам, свойствам и назначению.
19. Способы построения детерминированных математических моделей.
20. Аналитические и численные методы решения уравнений.
21. Сущность методов моделирования сложных систем.
22. Общие принципы и средства построения математических моделей процессов защиты информации.
23. Особенности построения математических моделей процессов защиты информации на основе экспериментальных данных.
24. Понятия корреляционного, регрессионного и дисперсионного анализов. Условия применимости статистического анализа.
25. Оценка достоверности и точности математических моделей.
26. Понятия целевой функции, оптимизируемых и фиксированных параметров, ограничений при оптимизации.
27. Понятие одномерной оптимизации. Глобальные и локальные экстремумы. Условия оптимума дифференцируемой функции одной переменной.
28. Понятие многомерной безусловной оптимизации. Условия оптимума дифференцируемой функции нескольких переменных.

Раздел «Организационно-правовая защита информации»

29. Общая характеристика организационных методов защиты информации.
30. Основные принципы организации системы безопасности объекта. Модель комплексной системы безопасности.
31. Классификация угроз информационной безопасности. Виды КУИ.
32. Основные направления организационной защиты информации на объекте.
33. Виды каналов несанкционированного доступа к информации. Их характеристика.
34. Концептуальная модель информационной безопасности.
35. Требования к построению систем безопасности предприятия.
36. Цели и задачи системы безопасности объекта. Виды объектов защиты.

37. Характеристика типовой структуры службы безопасности.
38. Случаи разглашение защищаемой информации.
39. Основные задачи службы безопасности объекта.
40. Характеристика функций службы безопасности объекта.
41. Права, обязанности и ответственность сотрудников службы безопасности.
42. Организация режима и охраны на объекте. Основные задачи.
43. Виды пропускных документов.
44. Порядок организации пропускного режима.
45. Организация охраны стационарных объектов.
46. Основные задачи охраны объектов.
47. Виды охраны стационарных объектов.
48. Характеристика деятельности отдела кадров объекта с позиции обеспечения защиты информации.
49. Способы пресечения разглашения защищаемой информации.
50. Организация инженерно-технической защиты объектов.
51. Характеристика организационных, организационно-технических и технических мероприятий защиты информации на объекте.
52. Организация аттестации защищенных помещений.
53. Организация работ по защите информации отдела обеспечения внешней деятельности.
54. Персонал фирмы и его роль в утечке информации.
55. Основные принципы организации профессионального отбора персонала.
56. Основные рекомендации при организации проверки и отбора кандидатов на работу в коммерческие предприятия.
57. Характеристика процесса увольнения кадров из коммерческих структур.
58. Особенности увольнения сотрудников, владеющих конфиденциальной информацией.
59. Основные этапы и процедуры профотбора персонала на коммерческие предприятия
60. Понятие режима секретности, его содержание и особенности.
61. РСО, ПДТК и их полномочия.
62. Порядок работы с секретными документами и изделиями.
63. Организация допуска лиц к секретным сведениям.
64. Организация засекречивания и рассекречивания сведений.
65. Организация работы с секретными документами.
66. Защита государственной тайны.
67. Организация защиты информации в кадровой службе.
68. Организация проведения служебных расследований по фактам утраты секретных документов.
69. Защита информации при проведении совещаний и переговоров.
70. Защита информации при работе с посетителями.
71. Характеристика информационно-аналитической работы.
72. Основные направления аналитической работы на объекте защиты.
73. Этапы выполнения аналитической работы.
74. Основные методы аналитической работы.

75. Общий подход к категорированию объектов охраны.
76. Организация защита информации при публикаторской и рекламной деятельности.
77. Основные направления и методы работы с персоналом, обладающим конфиденциальной информацией.
78. Основные этапы подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.
79. Лицензирование и сертификация в области защиты информации в РФ.
80. Лицензирование деятельности по защите информации.
81. Сертификация средств защиты информации
82. Коммерческая тайна и порядок её определения.
83. Организация работ с информацией, составляющей коммерческую тайну.
84. Организация и обеспечение защиты коммерческой тайны на предприятии.
85. Организация безопасности функционирования информационных систем.
86. Проведение аналитико-разведывательной работы.
87. государственная тайна и порядок отнесения к ней информации.
88. Характеристика действий по защите информации.
89. Противодействие НСД к информации.
90. Виды персональных данных в соответствии с ФЗ № 152 «О персональных данных»
91. Основные этапы создания СЗПДн на объекте.

Раздел «Инженерно-техническая защита информации»

92. Классификация информации, защищаемой техническими средствами.
93. Классификация демаскирующих признаков.
94. Принципы записи и съема информации с носителя.
95. Источники функциональных сигналов.
96. Побочные излучения и наводки. Основные понятия и классификации.
97. Характеристика основных источников информации.
98. Классификация акустоэлектрических преобразователей, создающих опасные сигналы.
99. Характеристика опасных сигналов.
100. Источники побочных высокочастотных колебании.
101. Виды паразитных связей.
102. Принципы возникновения паразитных наводок.
103. Виды угроз безопасности информации.
104. Характеристика органов добывания информации.
105. Задачи органов коммерческой разведки. Классификация видов технической разведки.
106. Характеристика видов агентурной и технической разведки.
107. Принципы добывания информации.
108. Технология добывания информации. Основные положения.
109. Основные составляющие процесса добывания информации.
110. Этапы технологии добывания информации.
111. Способы доступа к конфиденциальной информации.

112. Организация добывания информации без физического проникновения в контролируемую зону.
113. Организация доступа к источникам информации без нарушения государственной границы.
114. Особенности утечки информации по техническим каналам при эксплуатации ЭВМ.
115. Характеристики технических каналов утечки информации.
116. Структура канала передачи информации. Характеристика составляющих элементов.
117. Классификация технических каналов утечки информации.
118. Характеристика оптического КУИ.
119. Характеристика радиоэлектронного КУИ.
120. Классификация помех в технических каналах утечки.
121. Характеристика акустического КУИ.
122. Материально-вещественные каналы утечки информации.
123. Основные методы защиты информации техническими средствами.
124. Виды сокрытия информации.
125. Характеристика способов информационного сокрытия.
126. Дезинформирование. Способы. Характеристика. Основные особенности.
127. Энергетическое сокрытие.
128. Способы и средства ПДТР.
129. Способы контроля помещений на отсутствие закладных устройств.
130. Технические средства обеспечения охраны. Требования, задачи, состав.
131. Структура системы охраны объектов.
132. Способы защиты дверей и окон зданий и помещений.
133. естественные и искусственные преграды, используемые для охраны объектов.
134. Оснащение автоматизированных и автоматических контрольно-пропускных пунктов.
135. Способы и средства идентификации и аутентификации сотрудников.
136. шкафы, рабочие столы с закрываемыми на ключ ящиками, сейфы и хранилища. Виды, основные характеристики.
137. Классификация и основные элементы телевизионных систем наблюдения.
138. Компоненты и устройства ТСН.
139. Алгоритм выбора ТСН для объекта защиты.
140. Основные задачи, способы и средства инженерно-технической защиты информации.

Раздел «Программно-аппаратная защита информации»

141. Политика безопасности.
142. Матрица доступа.
143. Недостатки и достоинства схемы простой парольной аутентификации.
144. Биометрические методы идентификации и аутентификации.
145. Процедуры инициализации объекта информационной защиты.
146. Понятия идентификации и аутентификации.

147. Протоколы и алгоритмы идентификации.
148. Средства блокирования несанкционированного исследования и копирования информации КС.
149. Матричное управление доступом.
150. Функциональные блоки системы разграничения доступа к информации.
151. Функции диспетчера доступа.
152. Понятие ядра безопасности.
153. Проблемы создания высокоэффективной защиты от НСД.
154. Сравнительный анализ программных и аппаратных комплексов, рассчитанных на защиту персональных ЭВМ от несанкционированного доступа к ЭВМ, которые разграничивают доступ к информации и устройствам ПЭВМ.
155. Методы и средства обеспечения целостности и доступности информации.
156. Принципы организации защищенных систем управления.
157. Методы защиты ПК от несанкционированного доступа.
158. Группы методов защиты от угроз несанкционированного копирования.
159. Носители ключевой информации.
160. Понятие концепции иерархии ключей.
161. Распределение ключей.
162. Механизмы меток времени.
163. Методы противодействия дизассемблированию.
164. Методы противодействия трассировке программы.
165. Какие классы средств исследования программного обеспечения.
166. Функции должен выполнять инициализатора и деструктора.
167. Классификации компьютерных вирусов.
168. Группы антивирусного программного обеспечения.
169. Технологическая схема защиты.
170. Состав программного комплекса защиты.

Раздел «Криптографическая защита информации»

171. Исторические подходы к защите информации при передаче – физические методы, стенография, криптография.
172. Основные понятия и определения криптографии.
173. Классификация шифров.
174. Характер криптографической деятельности.
175. Эволюция шифров. Простейшие шифры и их свойства, композиции шифров, классические шифры, шифры гаммирования и колонной замены.
176. Алгебраические модели шифров.
177. Вероятностные модели шифров.
178. Математические модели открытых сообщений.
179. Криптографическая стойкость шифров.
180. Теоретико-информационный подход к оценке криптостойкости шифров.
181. Практическая стойкость шифров.
182. Имитостойкость шифров. Имитация и подмена сообщений.
183. Способы обеспечения имитостойкости.

184. Помехостойкость шифров.
185. Практические вопросы повышения надежности.
186. Виды симметричных шифров. Особенности программной и аппаратной реализации.
187. Принцип построения блочных шифров.
188. Современные блочные криптоалгоритмы.
189. Принцип построения поточных шифров.
190. Современные поточные криптоалгоритмы.
191. Режимы использования шифров.
192. Математические основы ассиметричной криптографии.
193. Примеры современных ассиметричных шифров.
194. Криптографические хэш-функции.
195. Задачи и особенности электронно-цифровой подписи.
196. Алгоритм цифровой подписи.
197. Симметричные (одноразовые) цифровые подписи.
198. Протокол распределения ключей.
199. Передача ключей с использованием симметричного и ассиметричного шифрования.
200. Открытое и предварительное распределение ключей.
201. Схемы распределения секрета.
202. Методы применения шифрования данных в локальных вычислительных сетях.
203. Обеспечение секретности данных при долгосрочном хранении
204. Задачи обеспечения секретности и целостности данных и ключей при краткосрочном хранении
205. Обеспечение секретности ключей при долгосрочном хранении
206. Защита от атак с использованием побочных каналов
207. Эллиптические кривые
208. Квантовая криптография

Раздел «Защита персональных данных»

209. Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных.
210. Методика определения актуальных угроз безопасности ИСПДн.
211. ФЗ № 152 «О персональных данных».
212. Модель угроз безопасности ИСПДн.
213. Постановление № 1119 « Об утверждении порядка требований к защите персональных данных при их обработке в информационных системах персональных данных».
214. Модель нарушителя.
215. Обеспечение контроля и надзора за выполнением требований по защите ПДн. Виды предусмотренных законодательством проверок.
216. Определения уровня защищенности ИСПДн
217. Типы информационных систем персональных данных
218. Виды программно-аппаратных средств защиты ИСПДн (примеры).

219. .Порядок определения наличия недекларированных возможностей в системной и прикладном ПО
220. Перечень организационно-распорядительных документов, регламентирующих защиту ПДн и ИСПДн на объекте.
221. Виды технических средств защиты ИСПДн (примеры).
222. Перечень нормативно-правовых актов, регламентирующих порядок наказаний за нарушение правил обработки персональных данных.
223. Выполнение мер по защите информационных систем персональных данных в соответствии с приказом № 21 ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
224. Модель угроз безопасности ИСПДн.
225. Перечень мер по защите ПДн, обрабатываемых без использования средств автоматизации.

Раздел «Управление интеллектуальной собственностью»

226. Понятие «интеллектуальная собственность»
227. Основные институты права интеллектуальной собственности;
228. Объекты интеллектуальной собственности, авторское право;
229. Особенности защиты служебной и коммерческой информации;
230. Общие признаки объектов интеллектуальной собственности;
231. Права авторов и патентообладателей интеллектуальной собственности;
232. Система правовой охраны интеллектуальной собственности;
233. Правовая охрана служебной и коммерческой тайны;
234. Институт права средств индивидуализации;
235. Международная патентная классификация, её структура;
236. Основные разделы патентного закона Российской Федерации;
237. Всемирная организация интеллектуальной собственности;
238. Гражданско-правовые способы защиты прав авторов и патентообладателей;
239. Международное сотрудничество в области промышленной собственности;
240. Право преждепользования, права патентообладателей.

12. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Изучение дисциплины инвалидами и лицами с ограниченными возможностями здоровья организуется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При проведении учебных занятий обеспечивается соблюдение следующих требований:

– учебные занятия проводятся для инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся в ходе учебных занятий;

– присутствие ассистента из числа работников БГТУ или привлеченных лиц, оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с педагогическим работником и т. п.);

– обучающиеся с учетом их индивидуальных особенностей могут пользоваться необходимыми им техническими средствами;

– материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже; наличие специальных кресел и других приспособлений).

Университетом созданы специальные условия для получения высшего образования обучающимися с ОВЗ:

1) для лиц с ограниченными возможностями здоровья по зрению:

– наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

– размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме (с учетом их особых потребностей) справочной информации о расписании учебных занятий (информация должна быть выполнена крупным рельефно-контрастным шрифтом (на белом или желтом фоне) и продублирована шрифтом Брайля);

– присутствие ассистента, оказывающего обучающемуся необходимую помощь;

– обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

– обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию организации;

2) для лиц с ограниченными возможностями здоровья по слуху:

– дублирование звуковой справочной информации о расписании учебных занятий визуальной (установка мониторов с возможностью трансляции субтитров (мониторы, их размеры и количество необходимо определять с учетом размеров помещения);

– обеспечение надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нару-

шения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения Университета, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, локальное понижение стоек-барьеров; наличие специальных кресел и других приспособлений).

13. ВОСПИТАТЕЛЬНАЯ РАБОТА

В соответствии с Федеральным законом от 31.07.2020г. № 304-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся» воспитание - «деятельность, направленная на развитие личности, создание условий для самоопределения и социализации обучающихся на основе социокультурных, духовно-нравственных ценностей и принятых в российском обществе правил и норм поведения в интересах человека, семьи, общества и государства, формирование у обучающихся чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению, взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации, природе и окружающей среде».

В учебном процессе воспитательная работа с обучающимися реализуется средствами учебных дисциплин.

Воспитательная деятельность в ходе преподавания дисциплины направленна на формирование у обучающегося системы убеждений, нравственных норм и общекультурных качеств, на оказание им помощи в жизненном самоопределении, нравственном, гражданском и профессиональном становлении, на создание условий для самореализации личности. Воспитательная работа также ориентирует обучающихся на будущую профессиональную деятельность, формируя не только личностные, но и профессионально значимые качества.

Воспитательные задачи во время учебных занятий выполняются в скрытой (контекстной) и открытой (целенаправленной) формах. Скрытая форма воспитательной работы представляет собой воздействие всего хода педагогического процесса на становление личностных качеств обучающихся. Например, соблюдение педагогическим работником трудовой дисциплины, демонстрация преданности науке, заинтересованность в успехе обучающихся, правильная речь, хорошие манеры и т. п. имеют положительное воспитательное значение и формируют у обучающихся добросовестность, исполнительность, трудолюбие, ответственность и другие положительные качества. Обучающиеся неосознанно перенимают данные черты у педагогического работника.

Воспитание в открытой форме – это целенаправленное воздействие содержанием учебной дисциплины на становление личности обучающегося. Например, решение проблем и исследовательская работа формируют у обуча-

ющихся умение аргументировать, самостоятельно мыслить, вкус к научному поиску, развивают творчество, профессиональные умения, и т. п.

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
Методы и системы защиты информации, информационная безопасность

(наименование дисциплины)

10.06.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Методы и системы защиты информации, информационная безопасность

(направленность (профиль)/ специализация образовательной программы)

высшее образование – подготовка кадров высшей квалификации

(уровень образования)

Исследователь. Преподаватель-исследователь

(квалификация, присваиваемая по специальности или направлению подготовки)

Очная

(форма обучения)

2020

(год набора)

1. Цель освоения дисциплины.

Целью освоения дисциплины является подготовка обучающихся к сдаче кандидатского экзамена по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

2. Место дисциплины в структуре ОПОП:

Дисциплина входит в обязательную часть образовательной программы и реализуется на 3 курсе в 6 семестре.

3. Компетенции, формируемые в результате освоения дисциплины

ОПК-1 – способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность;

ОПК-2 – способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности;

ОПК-3 – способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;

ОПК-4 – способность организовать работу коллектива по проведению научных исследований в области информационной безопасности;

ПК-1 – способность применять в научных исследованиях теорию и методологию обеспечения информационной безопасности и защиты информации;

ПК-2 – готовность ставить и решать инновационные задачи, связанные с разработкой моделей, методов и технических средств, повышающих эффективность эксплуатации существующих и создания новых средств защиты информации и обеспечения информационной безопасности с использованием глубоких фундаментальных и специальных знаний, аналитических методов и сложных моделей в условиях неопределенности;
ПК-3 – умение проводить анализ, самостоятельно ставить задачу исследования рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения;
ПК-4 – способность разрабатывать модели, методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.
ПК-5 – способность осуществлять педагогическую деятельность, в том числе по подготовке специалистов в области систем защиты информации и информационной безопасности.

4. Общая трудоемкость дисциплины
3 зачетные единицы (108 академических часа).

5. Форма (формы) промежуточной аттестации обучающихся
Экзамен.

6. Основные разделы дисциплины: 1) Теория и методология информационной безопасности; 2) Математическое моделирование процессов защиты информации; 3) Организационно-правовая защита информации; 4) Инженерно-техническая защита информации; 5) Программно-аппаратная защита информации; 6) Криптографическая защита информации; 7) Защита персональных данных; 8) Управление интеллектуальной собственностью.

7. Автор:
Рытов Михаил Юрьевич, доцент, к.т.н.