МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
подпись
«28» мая 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.30 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность 01.05.01 Фундаментальные математика и механика

Направленность (профиль) Фундаментальная математика и ее приложения
Вычислительная механика и компьютерный инжиниринг

Форма обучения очная

Квалификация Математик. Механик. Преподаватель

Краснодар 2021

Рабочая программа дисциплины информационная безопасность
составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки / специальности 01.05.01 Фундаментальные математика и механика (Фундаментальная математика и ее приложения)
код и наименование направления подготовки

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор _____
И.О. Фамилия, должность, ученая степень, ученое звание подпись

Рабочая программа дисциплины информационная безопасность
утверждена на заседании кафедры функционального анализа и алгебры
протокол № 9 «13» апреля 2021 г.
Заведующий кафедрой функционального анализа и алгебры
Барсукова В.Ю. _____
фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии
факультета/института математики и компьютерных наук
протокол № 3 «12» мая 2021 г.
Председатель УМК факультета/института Шмалько С.П. _____
фамилия, инициалы подпись

Рецензенты:
Сутокский В.Г. к.т.н., доцент кафедры наземного транспорта и механики КубГТУ
Лазарев В.А. д.п.н., зав. кафедрой теории функций КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассматривает задачи информатизации и защиты информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

1.2 Задачи дисциплины.

Задачи освоения дисциплины «Информационная безопасность»: получение базовых теоретических и исторических сведений о структуре информатизации, ее развитии, применении этих знаний на практике, перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации.

Изучение теоретических основ предмета: автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите; информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем; системы управления информационной безопасностью автоматизированных систем;

Развитие навыков разработки алгоритмов и практического решения прикладных задач информатизации. Сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности автоматизированных систем; подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к вариативной части Блока 1 "Дисциплины (модули)" учебного плана Б1.О.30

Курс «Информационная безопасность» продолжает, начатое на трех курсах математическое образование и студентов соответствующего направления подготовки. Знания, полученные в этом курсе, могут быть использованы в курсах защита операционных систем и баз данных, криптография, организационно-правовые методы защиты информации и др. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Дискретная математика», «Программирование», «Информатика», «Правоведение».

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ОПК-3. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ОПК-3.1 Имеет представление о принципах работы современных информационных технологий ОПК-3.2 Грамотно использует современные информационные технологии при решении задач профессиональной деятельности	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации; Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы	Всего часов	Семестры (часы)			
		9			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	**36**	**36**			
Занятия лекционного типа	18	18	-	-	-
Лабораторные занятия	18	18	-	-	-
Занятия семинарского типа (семинары, практические занятия)			-	-	-
	-	-	-	-	-
Иная контактная работа:					
Контроль самостоятельной работы (КСР)	4	2			
Промежуточная аттестация (ИКР)	0,2	0,3			
Самостоятельная работа, в том числе:	**7**	**7**			
Курсовая работа	-	-	-	-	-
Проработка учебного (теоретического) материала	4	4	-	-	-
Реферат	3	3	-	-	-
Контроль:	**26,7**	**26,7**			

Подготовка к экзамену		26,7	26,7			
Общая трудоемкость	**72**	**72**	**72**	**-**	**-**	**-**
	в том числе контактная работа	**38,3**	**38,3**			
	зач. ед	**2**	**2**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 7 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Виды информации и основные методы ее защиты. Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз ИБ РФ.	10	4		4	2
2	Организационно-правовые методы защиты информации	10	4		4	2
3	Программно-аппаратные методы защиты информации	10	4		4	2
4	Электронная Россия, электронный документооборот, универсальная электронная карта	13	6		6	1
	Итого по дисциплине:		18		18	7
	Контроль самостоятельной работы (КСР)	2				
	Промежуточная аттестация (ИКР)	0,7				
	Подготовка к текущему контролю	26,7				
	Общая трудоемкость по дисциплине	72				

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Виды информации и основные методы ее защиты. Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз ИБ РФ.	Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль ИБ в обеспечении национальной безопасности государства.	Р
2	Организационно-правовые методы защиты информации	Доктрина информационной безопасности. Сфера государственного управления. Финансово-экономические организации и предприятия. Информационная безопасность в силовых	Э

		структурах. Федеральные законы. Указы и Распоряжения Президента РФ, Постановления и Распоряжения Правительства РФ. Приказы и руководящие документы уполномоченных государственных органов.	
3	Программно-аппаратные методы защиты информации	Руководящие документы ФСТЭК (Гостехкомиссии), ФСБ, Минкомсвязи. ГОСТы по информатизации, биометрии и ТСЗИ. Защита периметра локальной сети. Средства наблюдения и предупреждения компьютерных вторжений. Защита от несанкционированного доступа.	Т
4	Электронная Россия, электронный документооборот, универсальная электронная карта	Закон о защите персональных данных - №152-ФЗ, закон об оказании государственных и муниципальных услуг №210-ФЗ. Проект УЭК. Государственная программа «Информационное общество». Переход госорганов на открытое программное обеспечение.	Р

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие.	Р
2	Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности	Р
3	Доктрина информационной безопасности. Сфера государственного управления. Финансово-экономические организации и предприятия. Информационная безопасность в силовых структурах.	Э
4	Федеральные законы. Указы и Распоряжения Президента РФ, Постановления и Распоряжения Правительства РФ. Приказы и руководящие документы уполномоченных государственных органов.	Р
5	Руководящие документы ФСТЭК (Гостехкомиссии), ФСБ, Минкомсвязи. ГОСТы по информатизации, биометрии и ТСЗИ.	Р
6	Защита периметра локальной сети. Средства наблюдения и предупреждения компьютерных вторжений. Защита от	Э

	несанкционированного доступа.	
7	Закон о защите персональных данных - №152-ФЗ, закон об оказании государственных и муниципальных услуг №210-ФЗ.	Р
8	. Проект УЭК. Государственная программа «Информационное общество». Переход госорганов на открытое программное обеспечение	Р

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т).

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Подготовка рефератов и научных сообщений	Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г.
2	Самостоятельное освоение теории	Рожков А.В. «Перечень электронных источников информации для самостоятельных работ по циклу дисциплин Информационная безопасность магистерской программы АМЗИ и рекомендации по его использованию». Методические указания, утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме с увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

3. Образовательные технологии.

Активные и интерактивные формы лекционных занятий, практических занятий, контрольных работ, тестовых заданий, типовых расчетов, докладов, сдача экзамена.

Вид занятия	Используемые интерактивные образовательные технологии
ЛЗ	Мультимедийная лекция-беседа: «Рекурсия. Быстрый алгоритм

	возведения в степень»
ПЗ	Дискуссия на тему: «Использование элементов алгебры в криптографии» с докладами-презентациями
ПЗ	Круглый стол на тему: «Теория чисел – алгоритмы проверки на простоту» с докладами-презентациями

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	Количество часов
3	Лекционные занятия	Тема Алгоритм проверки на простоту.	2
		Тема Алгоритм тестирования. Тест Эдуарда Люка	2
		Тема Тесты псевдопростоты.	4
		Тема Числа Кармайкла. Разложение чисел на простые числа.	2
	Лабораторные занятия	Дискуссия на тему: «. Метод локализации. Алгоритм пополнения.» с докладами-презентациями	2
		Круглый стол на тему: «Алгоритмы факторизации целых чисел.» с докладами-презентациями	2
		Мозговой штурм» («мозговая атака»): Базисы Грёбнера.	4
		Компьютерная симуляция: Решение системы полиномиальных уравнений	2
Итого:			18

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций со студентом при помощи электронной информационно-образовательной среды ВУЗа.

В рамках реализации компетентностного подхода предусматриваются следующие основные виды активных и интерактивных форм проведения учебных занятий, которые указываются в рабочих программах дисциплин, профессиональных модулей, практик в рамках которых они реализуются:

– применение электронных образовательных ресурсов;

– компьютерные симуляции;

– деловые и ролевые игры;

– индивидуальные и групповые проекты;

– анализ производственных ситуаций;

– разбор конкретных ситуаций;

– психологические и иные тренинги;

– групповые дискуссии и др.

Проблемная лекция. Преподаватель в начале и по ходу изложения учебного материала создает проблемные ситуации и вовлекает студентов в их анализ. Разрешая противоречия, заложенные в проблемных ситуациях, обучаемые самостоятельно могут прийти к тем выводам, которые преподаватель должен сообщить в качестве новых знаний.

Лекция с запланированными ошибками (лекция-провокация). После объявления темы лекции преподаватель сообщает, что в ней будет сделано определенное количество ошибок различного типа: содержательные, методические, поведенческие и т. д. Студенты в конце лекции должны назвать ошибки.

Лекция вдвоем. Представляет собой работу двух преподавателей, читающих лекцию по одной и той же теме и взаимодействующих как между собой, так и с аудиторией. В

диалоге преподавателей и аудитории осуществляется постановка проблемы и анализ проблемной ситуации, выдвижение гипотез, их опровержение или доказательство, разрешение возникающих противоречий и поиск решений.

Лекция-визуализация. В данном типе лекции передача преподавателем информации студентам сопровождается показом различных рисунков, структурно-логических схем, опорных конспектов, диаграмм и т. п. с помощью ТСО и ЭВМ (слайды, видеозапись, дисплеи, интерактивная доска и т. д.).

Лекция «пресс-конференция». Преподаватель просит студентов письменно в течение 2–3 минут задать ему интересующий каждого из них вопрос по объявленной теме лекции. Далее преподаватель в течение 3–5 минут систематизирует эти вопросы по их содержанию и начинает читать лекцию, включая ответы на заданные вопросы в ее содержание.

Лекция-диалог и лекция-дискуссия. Содержание подается через серию вопросов, на которые студенты должны отвечать непосредственно в ходе лекции.

Лекция с разбором конкретных ситуаций по форме организации похожа на лекцию-дискуссию, в которой вопросы для обсуждения заменены конкретной ситуацией, предлагаемой обучающимся для анализа в устной или письменной форме. Обсуждение конкретной ситуации может служить прелюдией к дальнейшей традиционной лекции и использоваться для акцентирования внимания аудитории на изучаемом материале.

Дискуссия – это публичное обсуждение или свободный вербальный обмен знаниями, суждениями, идеями или мнениями по поводу какого-либо спорного вопроса, проблемы. Ее существенными чертами являются сочетание взаимодополняющего диалога и обсуждения-спора, столкновение различных точек зрения, позиций.

Коллоквиум – вид учебных занятий, представляющий собой обсуждение под руководством преподавателя широкого круга проблем, например, относительно самостоятельного большого раздела лекционного курса или отдельных частей какой-либо конкретной темы. Он может включать вопросы и темы из изучаемой дисциплины, не включенные в темы практических и семинарских занятий. Коллоквиум может проводиться в форме индивидуальной беседы преподавателя со студентом или как групповое обсуждение.

«Круглый стол» – одна из форм организации дискуссии, в которой на равных участвуют 15–25 человек; в ходе нее происходит обмен мнениями между всеми участниками. Основное целевое назначение метода – обеспечение свободного, нерегламентированного обсуждения поставленных вопросов (тем) на основе постановки всех студентов в равное положение по отношению друг к другу. Как правило, перед участниками не стоит задача полностью решить проблему.

«Мозговой штурм» («мозговая атака») представляет собой разновидность групповой дискуссии, которая характеризуется отсутствием критики поисковых усилий, сбором всех вариантов решений, гипотез и предложений, рожденных в процессе осмысления какой-либо проблемы, их последующим анализом с точки зрения перспективы дальнейшего использования или реализации на практике. «Мозговой штурм» включает три этапа: подготовительный, этап генерирования идей, этап анализа и оценки идей. Продолжительность «мозгового штурма», как правило, не менее 1,5–2 часов.

Дебаты – формализованное обсуждение, построенное на основе выступлений участников – представителей двух или более противостоящих, соперничающих команд (групп). Данная образовательная технология основывается на умении анализировать

события, концентрироваться на обсуждаемой проблеме, собирать и обрабатывать информацию, творчески осмысливать возможности ее применения, определять собственную точку зрения по данной проблеме и защищать ее, организовывать взаимодействие в группе на основе соблюдения принятых правил и процедур совместной деятельности.

Разбор конкретных ситуаций (кейс-метод). Метод кейсов представляет собой изучение, анализ и принятие решений по ситуации, которая возникла в результате происшедших событий, реальных ситуаций или может возникнуть при определенных обстоятельствах в конкретной организации в тот или иной момент времени.

Ролевая игра – это эффективная отработка вариантов поведения в тех ситуациях, в которых могут оказаться обучающиеся (например, аттестация, защита или презентация какой-либо разработки, конфликт с однокурсниками и др.). Игра позволяет приобрести навыки принятия ответственных и безопасных решений в учебной ситуации. Признаком, отличающим ролевые игры от деловых, является отсутствие системы оценивания по ходу игры. Существенные признаки ролевой игры: – наличие игровой ситуации; – набор индивидуальных ролей; – несовпадение ролевых целей участников игры, принимающих на себя и исполняющих различные роли; – игровое взаимодействие участников игры; – проигрывание одной и той же роли разными участниками; – групповая рефлексия процесса и результата.

Деловая игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования тех систем отношений, которые характерны для этой деятельности, моделирования профессиональных проблем, реальных противоречий и затруднений, испытываемых в типичных профессиональных проблемных ситуациях. Существенные признаки деловой игры: – моделирование процесса труда (деятельности) руководителей и специалистов по выработке профессиональных решений; – наличие общей цели у всей группы; – распределение ролей между участниками игры; – различие ролевых целей при выработке решений; – взаимодействие участников, исполняющих те или иные роли; – групповая выработка решений участниками игры; – реализация цепочки решений в игровом процессе; – многоальтернативность решений; – наличие управляемого эмоционального напряжения

Тренинг – форма активного обучения, целью которого является передача знаний, развитие некоторых умений и навыков; метод создания условий для самораскрытия участников и самостоятельного поиска ими способов решения проблем.

Метод проектов – система организации обучения, при которой обучающиеся приобретают знания и умения в процессе самостоятельного планирования и выполнения постепенно усложняющихся практических заданий – проектов.

Компьютерная симуляция – это максимально приближенная к реальности имитация различных процессов (физических, химических, экономических, социальных и проч.) и (или) деятельности с использованием программного обеспечения образовательного назначения

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п.	Результаты обучения (в соответствии с п.	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация

	1.4)	1.4)		
1	ОПК-3.1 Имеет представление о принципах работы современных информационных технологий	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации;	Контрольная работа №1- Значение информационной безопасности для субъектов информационных отношений.	1.Сущность и понятие информационной безопасности. 2.Значение информационной безопасности для субъектов информационных отношений. 3.Место информационной безопасности в системе национальной безопасности.
2	ОПК-3.2 Грамотно использует современные информационные технологии при решении задач профессиональной деятельности	Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	Вопросы для устного (письменного) опроса по теме, разделу Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.	4.Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. 5. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию. 6. Каналы и методы несанкционированного доступа к конфиденциальной информации. 7 Методы правовой защиты информации. 8. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны. 9. Защита персональных данных. 10.Правовая основа допуска и доступа персонала к защищаемым сведениям.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов и заданий

1. ___ Сущность и понятие информационной безопасности.
2. ___ Значение информационной безопасности для субъектов информационных отношений.
3. ___ Место информационной безопасности в системе национальной безопасности.
4. ___ Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
5. ___ Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.
6. ___ Каналы и методы несанкционированного доступа к конфиденциальной информации.
7. Методы правовой защиты информации.
8. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны.
9. Защита персональных данных.
10. Правовая основа допуска и доступа персонала к защищаемым сведениям.
11. Система правовой ответственности за утечку информации и утрату носителей информации.
12. Правовые основы деятельности подразделений защиты информации.
13. Отрасли права, обеспечивающие законность в области защиты информации.
14. Основные законодательные акты, правовые нормы и положения.
15. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.
16. Основные правовые акты: закон об информатизации №149-ФЗ.
17. Основные правовые акты: закон о защите персональных данных №152-ФЗ.
18. Основные правовые акты: Доктрина информационной безопасности.
19. Интеллектуальная собственности и ее защита.
20. Принципы, силы, средства и условия организационной защиты информации.
21. Порядок засекречивания и рассекречивания сведений, документов и продукции.
22. Допуск и доступ к конфиденциальной информации и документам.
23. Организация внутри объектового и пропускного режимов на предприятиях.
24. История криптографии; классические шифры, шифры гаммирования.
25. Принципы построения криптографических алгоритмов.
26. Различие между программными и аппаратными реализациями шифров.
27. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
28. Криптографические хеш-функции.
29. Электронная подпись.
30. Криптографические протоколы.
31. Предмет и задачи программно-аппаратной защиты информации.
32. Идентификация субъекта, понятие протокола идентификации.
33. Основные подходы к защите данных от НСД.
34. Иерархический доступ к файлу.
35. Защита сетевого файлового ресурса, фиксация доступа к файлам.
36. Защиты программ от несанкционированного копирования.
37. Пароли и ключи, организация хранения ключей.
38. Защита программ от излучения.
39. Защита от отладки, защита от дизассемблирования.
40. Защита от разрушающих программных средств.
41. Антивирусы.
42. Межсетевые экраны.

Контрольная работа

Вариант 1

Применения и разработки шифровальных средств ……

Вариант 2

Применения электронной подписи.…….

Вариант 3

Модели, стратегии и системы обеспечения информационной безопасности.

Вариант 4

Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Вариант 5

Компьютерная система как объект информационной безопасности.

Реферат

Тематика рефератов

1. Общая характеристика методов и средств защиты информации.
2. Криптографические методы обеспечения информационной безопасности.
3. Защита в операционных системах.
4. Защита от вирусов.
5. Защита от вторжений.
6. Анализ нарушений безопасности в информационных системах.
7. Указ Президента РФ. Об утверждении перечня сведений конфиденциального характера от 06.03.1997 № 188 (ред. от 13.07.2015 № 357).
8. Указ Президента РФ. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена от 17.03.2008 № 351 (ред. от 22.05.2015 № 260).
9. Указ Президента РФ. О некоторых вопросах информационной безопасности Российской Федерации от 22.05.2015 № 260.
10. Указ Президента РФ. Об утверждении доктрины информационной безопасности Российской Федерации от 05.12.2016 № 486.
11. Обзор Сборника руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России, 1998 г.
12. Понятие атаки.
13. Типы угроз.
14. Классификация атак по основным механизмам реализации угроз.
15. Сетевые сканеры.
16. Особенности сетевого сканеров фирмы CISCO.
17. Встроенные средства защиты ОС Windows 8.
18. Встроенные средства защиты серверной ОС CentOS 7
19. Встроенные средства защиты клиентской ОС Debian.

Тест

Варианты 1-10

1. Методы и средства ограничения доступа к компонентам ЭВМ.
2. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
3. Методы и средства хранения ключевой информации
4. Защита программ от изучения.
5. Защита от разрушающих программных воздействий.
6. Защита от изменения и контроль целостности.
7. Проблемы обеспечения безопасности при удалённом доступе.

8. Протоколы аутентификации PAP и CHAP.

9. Протоколы аутентификации удалённого доступа в программных средствах Microsoft.

10. Система аутентификации и авторизации Kerberos.

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

1. Правовые основы деятельности подразделений защиты информации.
2. Отрасли права, обеспечивающие законность в области защиты информации.
3. Основные законодательные акты, правовые нормы и положения.
4. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.
5. Основные правовые акты: закон об информатизации №149-ФЗ.
6. Основные правовые акты: закон о защите персональных данных №152-ФЗ.
7. Основные правовые акты: Доктрина информационной безопасности.
8. Интеллектуальная собственности и ее защита.
9. Принципы, силы, средства и условия организационной защиты информации.
10. Порядок засекречивания и рассекречивания сведений, документов и продукции.
11. Допуск и доступ к конфиденциальной информации и документам.
12. Организация внутри объектового и пропускного режимов на предприятиях.
13. История криптографии; классические шифры, шифры гаммирования.
14. Принципы построения криптографических алгоритмов.
15. Различие между программными и аппаратными реализациями шифров.
16. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
17. Криптографические хеш-функции.
18. Электронная подпись.
19. Криптографические протоколы.
20. Предмет и задачи программно-аппаратной защиты информации.
21. Идентификация субъекта, понятие протокола идентификации.
22. Основные подходы к защите данных от НСД.
23. Иерархический доступ к файлу.
24. Защита сетевого файлового ресурса, фиксация доступа к файлам.
25. Защиты программ от несанкционированного копирования.
26. Пароли и ключи, организация хранения ключей.
27. Защита программ от излучения.
28. Защита от отладки, защита от дизассемблирования.
29. Защита от разрушающих программных средств.
30. Антивирусы.
31. Межсетевые экраны.

Критерии оценивания результатов обучения

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый	оценку «удовлетворительно» заслуживает студент, частично с

уровень «3» (удовлетворительно)	пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает формы допускает незначительные ошибки; студент умеет правильно объяснять материал, иллюстрируя его примерами

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, довольно ограниченный объем знаний программного материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

а) основная литература:

1. Нестеров С.А. Основы информационной безопасности. [Электронный ресурс]. - СПб.: Лань, 2021. - URL: https://e.lanbook.com/reader/book/165837
2. Новиков В.К. Информационное оружие – оружие современных и будущих войн, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2013. - URL: https://e.lanbook.com/book/11840

б) дополнительная литература:

1. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/126718/

2. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2017. - URL: https://e.lanbook.com/reader/book/1110975.3 Периодические издания:

Не предусмотрены

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);

9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля).

Согласно учебному плану дисциплины «Информационная безопасность» итоговой формой контроля является зачет. Для сдачи зачета студент должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3, выполнять домашние задания. Типы практических заданий на зачет соответствуют заданиям. Также на зачете студентам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы студента в течение семестра.

Важнейшим этапом курса является самостоятельная работа по дисциплине (модулю).

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете студентам достаточно использовать материал лекций. Весь этот теоретический материал содержится в учебных пособиях из списка основной литературы. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса. В случае затруднений, возникающих у студентов в процессе самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

7. 7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

При заполнении таблицы учитывать все виды занятий, предусмотренные учебным планом по данной дисциплине: лекции, занятия семинарского типа (практические занятия, лабораторные работы), а также курсовое проектирование, консультации, текущий контроль и промежуточную аттестацию.

При использовании лаборатории указать ее наименование «Лаборатория…».

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного	Мебель: учебная мебель Технические средства обучения:	

типа	экран, проектор, компьютер	
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	
Учебные аудитории для проведения лабораторных работ. Лаборатория…	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	
Учебные аудитории для курсового проектирования (выполнения курсовых работ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование:	

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Помещение для самостоятельной работы обучающихся (ауд._____)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность

1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2.	Семинарские занятия	Не предусмотрены
3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами с предустановленными GAP и Sage
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.