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
_____ Хагуров Т.А.
подпись
«29» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.40 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 2020

Рабочая программа дисциплины Информационная безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по специальности 01.05.01 Фундаментальные математика и механика

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор _____

Рабочая программа дисциплины Информационная безопасность утверждена на заседании кафедры функционального анализа и алгебры протокол № 9 «12» апреля 2019 г.
Заведующий кафедрой (разработчика) Барсукова В.Ю. _____

Рабочая программа обсуждена на заседании кафедры функционального анализа и алгебры протокол № 9 от «12» апреля 2019 г.
Заведующий кафедрой (выпускающей) Барсукова В.Ю. _____

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 2 «24» апреля 2019 г.
Председатель УМК факультета Титов Г.Н _____

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

Рабочая программа дисциплины Информационная безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по специальности 01.05.01 Фундаментальные математика и механика

Программу составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор _____

Рабочая программа дисциплины Информационная безопасность утверждена на заседании кафедры функционального анализа и алгебры протокол № 9 «10» апреля 2029 г.
Заведующий кафедрой (разработчика) Барсукова В.Ю. _____

Рабочая программа обсуждена на заседании кафедры функционального анализа и алгебры протокол № 9 «10» апреля 2029 г.
Заведующий кафедрой (разработчика) Барсукова В.Ю. _____

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 2 «30» апреля 2020 г.
Председатель УМК факультета Шмалько С.П._____

Рецензенты:

Сутокский В.Г. к.т.н., доцент кафедры наземного транспорта и механики КубГТУ
Лазарев В.А. д.п.н., профессор кафедры 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 обязательной части Блока 1 "Дисциплины (модули)" учебного плана Б1.О.40.

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 общекультурных/общепрофессиональных/профессиональных компетенций (ОПК/ПК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК-3	Способен самостоятельно создавать и грамотно использовать прикладные программные средства на основе современных информационных	содержание основных понятий по правовому обеспечению информационной безопасности;	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
2.	ПК-5	технологий и сетевых ресурсов вычислительных систем. Способен находить и извлекать актуальную научно-техническую информацию из электронных библиотек, реферативных журналов и т.п.	правовые способы защиты государственной тайны	системе действующего законодательства, в том числе с помощью систем правовой информации	научно-технической литературой в области символьных вычислений.

В результате освоения данной дисциплины обучающийся должен:

Знать:

о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства;

о методологии создания систем защиты информации;

о перспективных направлениях развития средств и методов защиты информации;

Уметь:

выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;

пользоваться современной научно-технической информацией по исследуемым проблемам и задачам;

применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований;

Владеть:

анализом информационной инфраструктуры государства;

формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 4 зач. ед. (144 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы	Всего часов	Семестры (часы)			
		7			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	**68**	**68**			
Занятия лекционного типа	34	34	-	-	-
Лабораторные занятия	34	34	-	-	-
Занятия семинарского типа (семинары, практические занятия)			-	-	-
	-	-	-	-	-
Иная контактная работа:					
Контроль самостоятельной работы (КСР)	4	4			
Промежуточная аттестация (ИКР)	0,3	0,3			
Самостоятельная работа, в том числе:					

Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		16	16	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		15	15	-	-	-
Реферат		5	5	-	-	-
Подготовка к текущему контролю				-	-	-
Контроль:						
Подготовка к экзамену		35,7	35,7			
Общая трудоемкость	144	144	-	-	-	-
	72,3	72,3				
	4	4				

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.	26	8	10		8
2	Организационно-правовые методы защиты информации	24	8	8		8
3	Программно-аппаратные методы защиты информации	28	10	8		10
4	Электронная Россия, электронный документооборот, универсальная электронная карта	26	8	8		10
	Итого по дисциплине:		**34**	**34**		**36**

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 структурах. Федеральные законы. Указы и Распоряжения Президента РФ, Постановления и Распоряжения Правительства РФ. Приказы и руководящие документы уполномоченных государственных органов.	Э
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 несанкционированного доступа.	Э
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 № 9 от 10.04.2020 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 № 9 от 10.04.2020 г.

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,

Перечень
электронных документов, которые могут быть представлены
в печатной форме с увеличенным шрифтом

1. Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
2. 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 30 августа 2017.
3. Бирюков А.А. Информационная безопасность: защита и нападение, 2-е изд. [Электронный ресурс]. – М.: ДМК Пресс, 2017. – URL: http://e.lanbook.com/view/book/93278/
4. Галатенко В.А. Стандарты информационной безопасности, 2-е изд. – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2016, 308 с.
5. Шаньгин В.Ф. Информационная безопасность. [Электронный ресурс]. – М.: ДМК Пресс, 2014. – URL: http://e.lanbook.com/view/book/50578/
6. Нестеров С.А. Основы информационной безопасности, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2018. - https://e.lanbook.com/book/103908.
7. Новиков В.К. Информационное оружие – оружие современных и будущих войн, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2013. - URL: http://e.lanbook.com/view/book/11840/
8. Рассолов М.М. Информационное право. [Электронный ресурс]. – М.: Проспект, 2015. - URL: http://e.lanbook.com/view/book/54523/

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 Тесты псевдопростоты.	4
		Тема Числа Кармайкла. Разложение чисел на простые	2

		числа.	
	Практические занятия	Дискуссия на тему: «. Метод локализации. Алгоритм пополнения.» с докладами-презентациями	4
		Круглый стол на тему: «Алгоритмы факторизации целых чисел.» с докладами-презентациями	6
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-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.

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.

4.1 Фонд оценочных средств для проведения текущего контроля.

Список теоретических вопросов (для подготовки к зачету)

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 внутриобъектового 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.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.
Список типовых алгоритмов (для самостоятельных и лабораторных занятий)

1. Применения и разработки шифровальных средств.
2. Применения электронной подписи.
3. Модели, стратегии и системы обеспечения информационной безопасности.
4. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
5. Компьютерная система как объект информационной безопасности.
6. Общая характеристика методов и средств защиты информации.
7. Криптографические методы обеспечения информационной безопасности.
8. Защита в операционных системах.
9. Защита от вирусов.
10. Защита от вторжений.
11. Анализ нарушений безопасности в информационных системах.
12. Указ Президента РФ. Об утверждении перечня сведений конфиденциального характера от 06.03.1997 № 188 (ред. от 13.07.2015 № 357).

13. 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).
14. Указ Президента РФ. О некоторых вопросах информационной безопасности Российской Федерации от 22.05.2015 № 260.
15. Указ Президента РФ. Об утверждении доктрины информационной безопасности Российской Федерации от 05.12.2016 № 486.
16. Обзор Сборника руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России, 1998 г.
17. Понятие атаки.
18. Типы угроз.
19. Классификация атак по основным механизмам реализации угроз.
20. Сетевые сканеры.
21. Особенности сетевого сканеров фирмы CISCO.
22. Встроенные средства защиты ОС Windows 8.
23. Встроенные средства защиты серверной ОС CentOS 7
24. Встроенные средства защиты клиентской ОС Debian.

Примерные темы реферативных докладов

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.

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

5.1 Основная литература:

1. Бирюков А.А. Информационная безопасность: защита и нападение, 2-е изд. [Электронный ресурс]. – М.: ДМК Пресс, 2017. – URL: http://e.lanbook.com/view/book/93278/
2. Нестеров С.А. Основы информационной безопасности, 5-е изд. [Электронный ресурс]. - СПб.: Лань, 2019. - URL: https://e.lanbook.com/reader/book/114688

5.2 Дополнительная литература:

1. Новиков В.К. Информационное оружие – оружие современных и будущих войн, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2013. - URL: http://e.lanbook.com/view/book/11840/
2. Рассолов М.М. Информационное право. [Электронный ресурс]. – М.: Проспект, 2015. - URL: http://e.lanbook.com/view/book/54523/

1.3. Периодические издания:

Не предусмотрены

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

7. 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.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

8.2 Перечень необходимого программного обеспечения.

8.2 Перечень необходимого программного обеспечения.

а) перечень лицензионного программного обеспечения:

№	Учебный год	Произво-дитель	Наименование	Лицензионный договор	Дата заключения договора
1	2018-2019	Microsoft	Microsoft Windows 8, 10	№73–АЭФ/223-ФЗ/2018 Соглашение Microsoft ESS 72569510	XX.11.2018
2	2018-2019	Microsoft	Microsoft Office Professional Plus	№73–АЭФ/223-ФЗ/2018 Соглашение Microsoft ESS 72569510	XX.11.2018
3	2018-2019	Microsoft	Microsoft Office 365 Professional Plus	№73–АЭФ/223-ФЗ/2018 Соглашение Microsoft ESS 72569510	XX.11.2018
4	2017-2018	Microsoft	Windows 8, 10	№77-АЭФ/223-ФЗ/2017 Соглашение Microsoft ESS 72569510	03.11.2017
5	2017-2018	Microsoft	Microsoft Office Professional Plus	№77-АЭФ/223-ФЗ/2017 Соглашение Microsoft ESS 72569510	03.11.2017
6	2017-2018	Microsoft	Microsoft Visio	№77-АЭФ/223-ФЗ/2017 Соглашение Microsoft ESS 72569510	03.11.2017
7	2018-2019	Новые	МойОфис Частное	№02-еп/223-ФЗ/2018	29.01.2018

		облачные технологии	Облако		
8	2018-2019	Новые облачные технологии	МойОфис Стандартный	№02-еп/223-ФЗ/2018	29.01.2018
9	2018-2019	WolframResearch	Mathematica		
10	2017-2018	COMSOL	COMSOL	№51-АЭФ/223-2017	17.07.2017
11	2017-2018	COMSOL	LiveLink for MATLAB	№51-АЭФ/223-2017	17.07.2017
12	2017-2018	StatSoft	Statistica	№74-АЭФ/44-ФЗ/2017	05.12.2017
13	2016-2017	MapleSoft	Maple 18	№127-АЭФ/2014	29.07.2014
14	2016-2017	ABBYY	FineReader 12	№127-АЭФ/2014	29.07.2014
15	2016-2017	Embarcadero	RAD Studio XE6	№127-АЭФ/2015	30.07.2014
16	2016-2017	Corel	CorelDRAW Graphics Suite X7	№127-АЭФ/2015	30.07.2014
17	2016-2017	ABBYY	PDF Transformer+	№127-АЭФ/2014	29.07.2014
18	2016-2017		PROMT Professional 9.5	№127-АЭФ/2014	29.07.2014
19	2016-2017	Mathworks	MATLAB Wavelet Toolbox	№127-АЭФ/2014	29.07.2014
20	2016-2017	Mathworks	Simulink, Signal Processing Toolbox	№127-АЭФ/2014	29.07.2014

в) Перечень свободно распространяемого программного обеспечения

№	**Перечень свободно распространяемого программного обеспечения**
1.	Пакет компьютерной алгебры Sage 8.3. Официальный сайт http://sagemath.org/
2.	Пакет компьютерной алгебры Gap4r9p3. Официальный сайт http://www.gap-system.org/
3.	Пакет компьютерной алгебры PARI/GT 2.11. Официальный сайт http://pari.math.u-bordeaux.fr/
4.	Библиотека для работы с большими целыми числами GMP 6.1.2. Официальный сайт https://gmplib.org/
5.	Язык программирования Python. Официальный сайт https://www.python.org/
6.	Язык программирования Julia. Официальный сайт http://julialang.org/
7.	Язык программирования Cython. Официальный сайт http://cython.org/
8.	Компилятор PyPy, оптимизирующий код Python и Cython. Официальный сайт http://pypy.org/
9.	Python в облаке, интегрированная среда разработки Anaconda. Официальный сайт https://store.continuum.io/cshop/anaconda/
10.	Математические пакеты Python, проект SciPy. Официальный сайт http://www.scipy.org/
11.	Клиентская ОС Debian 9.5. Официальный сайт https://www.debian.org/index.ru.html
12.	Издательская система LaTeX/MiKTeX 2.9. Официальный сайт http://www.miktex.org/
13.	Утилиты Руссиновича https://technet.microsoft.com/ru-ru/library/bb545021.aspx
14.	Анализ защищенности сети Kali Linux 2018.3. https://www.kali.org/
15.	Анализ защищенности сети Snort 3.0. Официальный сайт https://www.snort.org/
16.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт

	https://www.openoffice.org/ru/

8.3 Перечень информационных справочных систем:

1. http://www.pravo.gov.ru – официальный портал правовой информации
2. http://www.government.ru - интернет-портал Правительства РФ
3. http://graph.document.kremlin.ru - раздел «Документы» портала Президента России
4. http://minsvyaz.ru/ru - сайт Минкомсвязи РФ
5. http://www.rsoc.ru - сайт Федеральной службы Роскомнадзор
6. http://www.scrf.gov.ru – сайт Совета безопасности РФ
7. http://base.consultant.ru – сайт правовой информации «Консультант+»
8. http://www.fstec.ru – официальный сайт ФСТЭК России
9. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/
10. Электронная библиотека http://gen.lib.rus.ec/

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю).

№	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.

РЕЦЕНЗИЯ

на рабочую программу дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность 01.05.01 Фундаментальные математика и механика
Направленность Математическое моделирование

Рабочая программа дисциплины Информационная безопасность для студентов направленность Математическое моделирование составлена доктором физико-математических наук, профессором кафедры функционального анализа и алгебры факультета математики и компьютерных наук Кубанского государственного университета Рожковым А.В.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования (ФГОС ВО) по специальности 01.05.01 Фундаментальные математика и механика. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Содержание рабочей программы соответствует актуальным направлениям развития теории информационной безопасности электронных информационных систем. 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 действующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем.

Рабочая программа дисциплины Информационная безопасность для студентов направленность Математическое моделирование сочетает теоретическую и практические части. Получение базовых практических сведений и навыков о структуре и алгоритмах символьных математических вычислений.

Считаю, что рабочая программа дисциплины Информационная безопасность для студентов направленность Математическое моделирование может быть рекомендована для подготовки студентов специальности 01.05.01 Фундаментальные математика и механика.

Доктор педагогических наук,
заведующий кафедрой теории функций
ФГБОУ ВО «КубГУ»

В.А. Лазарев