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

«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.02 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Направление подготовки 01.04.01 Математика

Направленность (профиль) Алгебраические методы защиты информации

Форма обучения очная

Квалификация магистр

Краснодар 2024

Рабочая программа дисциплины Теоретические основы компьютерной безопасности
составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки
01.04.01 Математика Алгебраические методы защиты информации
код и наименование направления подготовки

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

Рабочая программа дисциплины Теоретические основы компьютерной безопасности утверждена на заседании кафедры функционального анализа и алгебры протокол № 12 «07» мая 2024 г.
Заведующий кафедрой функционального анализа и алгебры
Барсукова В.Ю.

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 3 «14» мая 2024 г.
Председатель УМК факультета Шмалько С.П.

Рецензенты:
Сутокский В.Г. к.т.н., доцент кафедры наземного транспорта и механики КубГТУ
Лежнев А.В. к.ф.-м.н., зав. кафедрой математических и компьютерных методов КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассматривает теоретические и технологические 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 Теоретические основы компьютерной безопасности: обучить магистров принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных автоматизированных систем (АС), а также содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления. Знания и практические навыки, полученные из курса «Теоретические основы компьютерной безопасности», используются обучаемыми при изучении естественнонаучных дисциплин.

Знания и умения, приобретенные в ходе изучения курса «Теоретические основы компьютерной безопасности» используются обучаемыми при разработке дипломных работ.

Задачи дисциплины – дать основы:

- устройства и принципов функционирования защищенных АС,
- методологии проектирования и построения защищенных АС,
- критериев и методов оценки защищенности АС,
- средств и методов несанкционированного доступа (НСД) к информации АС.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина Теоретические основы компьютерной безопасности относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана Б1.В.02.

Данная дисциплина как составная часть науки «Информационное право» - правового фундамента информационного общества, а также как раздел дискретной математики и теории управления, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров.

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

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-1 Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	
ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области ПК-1.3 Самостоятельно и корректно решает стандартные задачи фундаментальной и прикладной математики ПК-1.4 Имеет навыки решения	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований	
ПК-4 Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	
ПК-4.1 Умеет применять и реализовывать математически сложные алгоритмы в современных программных комплексах ПК-4.2 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике и естественных науках ПК-4.3 Демонстрирует умение отбора среди существующих методов наиболее подходящие для решения конкретной прикладной задачи	Уметь: проводить анализ АС с точки зрения обеспечения компьютерной безопасности, разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы, применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС, реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС; Владеть навыками: работы с АС распределенных вычислений и обработки информации; работы с документацией АС, использования критериев оценки защищенности АС, построения формальных моделей систем защиты информации АС.

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)			
		1			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	**32**	**32**			
Занятия лекционного типа	16	16	-	-	-
Лабораторные занятия	16	16	-	-	-
Занятия семинарского типа (семинары, практические занятия)			-	-	-
	-	-	-	-	-
Иная контактная работа:					
Контроль самостоятельной работы (КСР)					
Промежуточная аттестация (ИКР)	0,3	0,3			

Самостоятельная работа, в том числе:		**85**	**85**			
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		40	40	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		30	30	-	-	-
Реферат		7	7	-	-	-
Подготовка к текущему контролю		8	8	-	-	-
Контроль:						
Подготовка к экзамену		26,7	26,7			
Общая трудоемкость	**час.**	**144**	**144**	**-**	**-**	**-**
	в том числе контактная работа	**32,3**	**32,3**			
	зач. ед	**4**	**4**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 1 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Структура теории компьютерной безопасности.		4		4	20
2	Методология построения систем защищенных АС		4		4	20
3	Политика безопасности.		4		4	20
4	Основные критерии защищенности АС. Классы защищенности АС.		4		4	25
	Итого по дисциплине:		16		16	85

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

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Структура теории компьютерной безопасности.	Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров	Р

		информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации. Основные виды атак на АС. Классификация основных атак на АС и вредоносных программ.	
2	Методология построения систем защищенных АС	Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации. Построение системы защиты от угрозы доступности информации. Эксплутационно-технологические меры защиты. Защита от сбоев программно-аппаратной среды. Защита семантического анализа и актуальности информации.Построение системы защиты от угрозы раскрытия параметров информационной системы. Сокрытие характеристик носителей. Мониторинг использования систем защиты. Защита параметров представления и содержания информации.Методология обследования и проектирования защиты АС. Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ).	Э
3	Политика безопасности.	Понятие политики безопасности. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы. Эквивалентные подходы к определению	Т

		безопасности модели Белла-Лападулы.	
4	Основные критерии защищенности АС. Классы защищенности АС.	Основные критерии оценки защищенности АС. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем. Стандарты по оценки защищенности АС.Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).Основные требования к системам защиты в TCSEC. Классы защиты TCSEC.Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты.Единые критерии безопасности информационных технологий (Common Criteria).Основные положения «Единых критериев». Требования безопасности. Профили защиты.	Р

2.3.2 Занятия семинарского типа.

Не предусмотрены

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.			
2.			

2.3.3 Лабораторные занятия.

№	Наименование практических работ	Форма текущего контроля
1	3	4
1	Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ.	Р
2	Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информационной безопасности.	Р
3	Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.	Э
4	Защита содержания информации. Основные виды атак на АС.	Р
5	Классификация основных атак на АС и вредоносных программ.	Р
6	Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды.	Э
7	Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации.	Р
8	Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ	Р

	информационных каналов. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы	

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 № 12 от 7 мая 2024 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 № 12 от 7 мая 2024.

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.
2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.
3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.
4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.
5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.
6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 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,

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 экзамену)

1. Модели ценности информации.
2. Примеры реализации систем парольной защиты и их анализ.
3. Алгоритмическая неразрешимость проблемы безопасности с использованием модели *HRU*.
4. Правила передачи прав доступа в модели *Take-Grant*.
5. Расширенная модель *Take-Grant*.
6. Анализ путей возникновения информационных каналов.
7. Примеры использования модели контроля информационных потоков модели Белла-Лападула для построения системы защиты.
8. Классификация защищенности операционных систем *Unix, Microsoft Windows* с использованием стандартов *TCSEC*.
9. Основные виды вредоносных программ и методы борьбы с ними.
10. Классификация угроз информации в операционных системах, базах данных, системах электронной почты.
11. Методы обеспечения целостности программно-аппаратной среды. Основные методы защиты памяти.
12. Построение систем защиты с помощью матрицы доступа.
13. Практические методы разработки и реализации политики безопасности.
14. Сравнительный анализ стандартов оценки безопасности компьютерных систем TCSEC, руководящих документов Гостехкомиссии РФ и «Единых критериев». Вредоносный программный код.
15. Классификация вирусов по способу загрузки.
16. Руководящие документы ФСТЭК по защите от вирусов.
17. Сертифицированные антивирусные средства и алгоритмы их работы.
18. Межсетевые экраны. Выбор межсетевого экрана.
19. Настройка служб и администрирование межсетевого экрана.
20. Встраивание межсетевого экрана в систему защиты локальной сети.
21. Требования к защите автоматизированных систем от НСД.
22. Матрица доступа и нормативные акты, регламентирующие ее создание.
23. Выбор и реализация политики сетевой безопасности на предприятии.
24. Программно-аппаратные и организационно-правовые механизмы защиты корпоративной информации.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Список типовых алгоритмов (для самостоятельных занятий)

1. Техническое воздействие на обработку информации.
2. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.
3. Виды и особенности деятельности по защите информации.
4. Лицензирование деятельности по защите информации.
5. Виды уязвимости информации.

6. Виды уязвимости информации и формы ее проявления.
7. Каналы и методы несанкционированного доступа к конфиденциальной информации.
8. Технические методы защиты от НСД.
9. Программно-аппаратные методы защиты информации.
10. Методологические подходы к защите информации.
11. Принципы организации защиты информации.
12. Объекты защиты.
13. Виды защиты.
14. Классификация методов и средств защиты информации.
15. Кадровое и ресурсное обеспечение защиты информации.
16. Системы защиты информации.
17. Анализ Федерального закона. Об информации, информационных технологиях и о защите информации от 27.07.2006 № 149-ФЗ
18. Анализ причин выхода Указа Президента РФ. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации от 15.01.2013 № 31с.
19. Анализ Федерального закона. О федеральной службе безопасности от 03.04.1995 № 40-ФЗ.
20. Обзор Сборника руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России, 1998 г.

Примерные темы реферативных докладов

1. Угрозы для изолированного компьютера.
2. Виды противников или «нарушителей».
3. Встроенные средства защиты операционной системы.
4. Матрица доступа.
5. Парольная политика.
6. Угрозы в открытых сетях.
7. Классические и современные методы взлома интрасетей.
8. Уязвимости основных структурно-функциональных элементов.
9. Сетевые анализаторы трафика.
10. Политика безопасности и сертифицированные средства защиты.
11. Защита узлов компьютерной сети.
12. Основные факторы и угрозы, влияющие на безопасность информационных ресурсов.
13. Типовые средства защиты информации и способы их применения.
14. Демилитаризованная зона.
15. Разграничение прав доступа.
16. Системы контроля целостности.
17. Антивирусные средства.
18. Требования к программно-аппаратной защите информации.
19. Нормативные требования к средствам защиты уполномоченных государственных органов.
20. Процедура сертификации средств защиты.
21. Аудит защищенности информационной системы.

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 уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает студент, частично с 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:

1. Прохорова О.В. Информационная безопасность и защита информации, 5-е изд. [Электронный ресурс]. – СПб.: Лань, 2024. - https://reader.lanbook.com/book/385082
2. Нестеров С.А. Основы информационной безопасности, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2024. - URL: https://reader.lanbook.com/book/370967

5.2 Дополнительная литература:

1. Никифоров С.Н. Методы защиты информации. Защита от внешних вторжений, 5-е изд. [Электронный ресурс]. - СПб.: Лань, 2023. - https://reader.lanbook.com/book/288974
2. Лозовецкий В.В., Комаров Е.Г., Лебедев В.В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей: Учебное пособие для вузов, 2-е изд. [Электронный ресурс]. – СПб.: Лань, 2024. - URL: https://e.lanbook.com/reader/book/ 397355

5.3 Периодические издания:

Не предусмотрены

6. 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/

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.

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 типа	Мебель: учебная мебель Технические средства обучения: 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.

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

Согласно учебному плану дисциплины «Алгебраическая алгоритмика» итоговой формой контроля является зачет. Для сдачи зачета магистр 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 магистрам предлагаются и теоретические задания, состоящие в письменном

ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы магистра 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 магистрам 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.

РЕЦЕНЗИЯ

на рабочую программу дисциплины

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Направление подготовки 01.04.01 Математика
Направленность Алгебраические методы защиты информации

Рабочая программа дисциплины Теоретические основы компьютерной безопасности для магистров направленность «Алгебраические методы защиты информации» 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 направлению подготовки 01.04.01 Математика. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Содержание рабочей программы – это построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. В программе отражены все основные темы информационной безопасности.

Рабочая программа дисциплины Теоретические основы компьютерной безопасности для магистров направленность «Алгебраические методы защиты информации» сочетает теоретическую и практические части, что способствует более глубокому усвоению материала. Предложенные задания научно-исследовательского плана направлены на развитие практических навыков решения задач по направлению защита информации.

Считаю, что рабочая программа дисциплины Теоретические основы компьютерной безопасности для магистров направленность «Алгебраические методы защиты информации» может быть рекомендована для подготовки магистров направления подготовки 01.04.01 Математика.

Кандидат технических наук,
доцент кафедры наземного транспорта и механики
ФГБОУ ВО «КубГТУ»

В.Г. Сутокский