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
«31» мая 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.28 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 02.03.01 Математика и компьютерные науки

Направленность (профиль) Алгебра, теория чисел и дискретный анализ
Вычислительные, программные, информационные системы и компьютерные технологии
Математическое и компьютерное моделирование

Форма обучения очная

Квалификация бакалавр

Краснодар 2019

Рабочая программа дисциплины Информационная безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.01 Математика и компьютерные науки

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 от «12» апреля 2019 г.
Заведующий кафедрой (разработчика) Барсукова В.Ю. _____

Рабочая программа обсуждена на заседании кафедры вычислительной математики и информатики, протокол № 13 от «18» апреля 2019 г.
Заведующий кафедрой (выпускающей) Гайденко С. В. _____

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 2 «24» апреля 2019 г.
Председатель УМК факультета _Титов Г.Н_____ _____
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 обязательной части Блока 1 "Дисциплины (модули)" учебного плана Б1.О.28.

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 общепрофессиональных компетенций (ОПК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК-5	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, в том числе отечественного производителя, и с учетом основных требований информационной безопасности	содержание основных понятий по правовому обеспечению информационной безопасности; правовые способы защиты государственной тайны	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной 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 2 зач. ед. (72 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы	Всего часов	Семестры (часы)			
		8			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	**48**	**48**			
Занятия лекционного типа	24	24	-	-	-
Лабораторные занятия	24	24	-	-	-
Занятия семинарского типа (семинары, практические занятия)			-	-	-

		-	-	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		4	4			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:						
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		3	3	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		2	2	-	-	-
Подготовка к текущему контролю		2,8	2,8	-	-	-
Контроль:						
Подготовка к зачету		-	-			
Общая трудоемкость	**час.**	**72**	**72**	**-**	**-**	**-**
	в том числе контактная работа	**52,2**	**52,2**			
	зач. ед	**2**	**2**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 8 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.	16	6		6	4
2	Организационно-правовые методы защиты информации	16	6		6	5
3	Программно-аппаратные методы защиты информации	18	6		6	4
4	Электронная Россия, электронный документооборот, универсальная электронная карта	16,8	6		6	5,8
	Итого по дисциплине:		**24**		**24**	**19,8**

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 руководя-	Р

	щие документы уполномоченных государственных органов.	
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 12 апреля 2019 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 12 апреля 2019 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. Образовательные технологии.

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

Семестр	**Вид занятия**	**Используемые интерактивные образовательные технологии**	**Количество часов**
7	Лабораторные занятия	Дискуссия на тему: «Метод локализации. Алгоритм пополнения» с докладами-презентациями	6
		Дискуссия на тему: «Алгоритмы факторизации целых чисел.» с докладами-презентациями	6
		Дискуссия на тему: «Использование элементов алгебры в криптографии» с докладами-презентациями	6
Итого:			18

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

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.
Общие вопросы, которые выносятся на дискуссию:

1. Составления плана решения задачи.
2. Определение возможных способов решений задачи.
3. Выбор среди рассматриваемых алгоритмов наиболее рационального.
4. Самостоятельное составление студентами алгоритмов решения заданий по теме, характеризующих глубину понимания соответствующего материала.

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 кон-

фиденциальности.

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.

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. Нестеров С.А. Основы информационной безопасности, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2018. – URL. https://e.lanbook.com/reader/book/103908/#1

2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: https://e.lanbook.com/reader/book/70724/#1

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: https://e.lanbook.com/reader/book/11840/#1
2. Аверченков В.И. Аудит информационной безопасности, 2-е изд. [Электронный ресурс] – М.: Издательство "ФЛИНТА", 2011. – URL: https://e.lanbook.com/reader/book/20195/#1

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.

а) перечень лицензионного программного обеспечения:

№	Перечень лицензионного программного обеспечения
1.	Microsoft office
2.	Comsol
3.	Free Pascal
4.	Visual Studio
5.	PROMT
6.	MS Windows 10 (x64)
7.	MS Office 2013, MS

8.	Office 2010, 7Zip

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
4.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
5.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
6.	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

Направление подготовки 02.03.01 Математика и компьютерные науки
Направленность Алгебра, теория чисел и дискретный анализ

Рабочая программа дисциплины Информационная безопасность для студентов направленность Алгебра, теория чисел и дискретный анализ 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 02.03.01 Математика и компьютерные науки. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Содержание рабочей программы. 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; системы управления информационной безопасностью автоматизированных систем.

Рабочая программа дисциплины Информационная безопасность для студентов направленность Алгебра, теория чисел и дискретный анализ 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 Алгебра, теория чисел и дискретный анализ может быть рекомендована для подготовки студентов направления подготовки 02.03.01 Математика и компьютерные науки.

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



В.А. Лазарев

РЕЦЕНЗИЯ

на рабочую программу дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 02.03.01 Математика и компьютерные науки
Направленность Алгебра, теория чисел и дискретный анализ

Рабочая программа дисциплины Информационная безопасность для студентов направленность Алгебра, теория чисел и дискретный анализ 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 02.03.01 Математика и компьютерные науки. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Студенты, освоившие дисциплину Информационная безопасность должны 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.

Рабочая программа дисциплины Информационная безопасность для студентов направленность Алгебра, теория чисел и дискретный анализ 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 Информационная безопасность для студентов направленность Алгебра, теория чисел и дискретный анализ может быть рекомендована для подготовки студентов направления подготовки 02.03.01 Математика и компьютерные науки.

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



В.Г. Сутокский