Министерство образования и науки 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

_____ Иванов А.Г.

«01» июля 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.06.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 01.03.01 Математика

Направленность (профиль): Математическое моделирование;
Преподавание математики и информатики

Программа подготовки академическая

Форма обучения очная

Квалификация (степень) выпускника бакалавр

Краснодар 2016

Рабочая программа дисциплины Информационная безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.03.01 Математика

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

Рабочая программа дисциплины Информационная безопасность утверждена на заседании кафедры функционального анализа и алгебры, протокол № 1 «30» августа 2016 г.
Заведующий кафедрой (разработчика) Барсукова В.Ю. _____
фамилия, инициалы подпись

Рабочая программа обсуждена на заседании кафедры (выпускающей) функционального анализа и алгебры протокол № 1 «30» августа 2016 г.
Заведующий кафедрой (выпускающей) Барсукова В.Ю. _____

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 1 «1» сентября 2016 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 вариативной части Блока 1 "Дисциплины (модули)" учебного плана Б1.В.ДВ.06.01.

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)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК-2	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением	содержание основных понятий по правовому обеспечени ю информацио	отыскивать необходимые нормативные правовые акты и информацион но-правовые	использовани я библиотеки алгоритмов и пакетов расширения; поиска и использовани

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	нной безопасности; правовые способы защиты государственной тайны	нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	я современной научно-технической литературой в области символьных вычислений.
2	ПК-7	способностью использовать методы математического и алгоритмического моделирования при анализе управленческих задач в научно-технической сфере, в экономике, бизнесе и гуманитарных областях знаний			

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):	**36**	**36**			
Занятия лекционного типа			-	-	-
Лабораторные занятия	36	36	-	-	-

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		8	8	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		8	8	-	-	-
Реферат		4	4	-	-	-
Подготовка к текущему контролю		15,8	15,8	-	-	-
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час.**	**72**	**72**	**-**	**-**	**-**
	в том числе контактная работа	**36,2**	**36,2**			
	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			8	8
2	Организационно-правовые методы защиты информации	16			8	8
3	Программно-аппаратные методы защиты информации	20			10	10
4	Электронная Россия, электронный документооборот, универсальная электронная карта	19,8			10	9,6
	Итого по дисциплине:				36	35,8

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.

Не предусмотрено

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 № 1 от 31 августа 2017 г.
2	Самостоятельное освоение теории	Рожков А.В. «Перечень электронных источников информации для самостоятельных работ по циклу дисциплин Информационная безопасность магистерской программы АМЗИ и рекомендации по его использованию». Методические указания, утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017.

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

Для лиц с нарушениями зрения:

– в печатной форме с увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

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 31 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 31 августа 2017.

3. Образовательные технологии.

Активные и интерактивные формы, лекции, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и зачет. В течение семестра студенты решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый студент готовит реферативный доклад по одной из ниже научных тем. Зачет выставляется после выполнения определенного количества (практических и теоретических) заданий контрольных работ и отчета по реферативному докладу. В случае невыполнения какого-то из приведенных требований, студенту для сдачи зачета предлагаются по усмотрению преподавателя некоторые практические и теоретические задания, подобные предложенным ниже.

К образовательным технологиям также относятся интерактивные методы обучения. Интерактивность подачи материала по дисциплине «Информационная безопасность» предполагает не только взаимодействия вида «преподаватель - студент» и «студент -

преподаватель», но и «студент - студент». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения студентами реферативных докладов (возможно в виде презентации).

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 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

5.3 Периодические издания:

Не предусмотрены

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

Интернет-ресурсы:

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/

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.

№	**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

№	**Перечень свободно распространяемого программного обеспечения**
1.	Язык программирования Python. Официальный сайт https://www.python.org/
2.	Язык программирования Julia. Официальный сайт http://julialang.org/
3.	Язык программирования Cython. Официальный сайт http://cython.org/
4.	Компилятор PyPy, оптимизирующий код Python и Cython. Официальный сайт http://pypy.org/
5.	Python в облаке, интегрированная среда разработки Anaconda. Официальный сайт https://store.continuum.io/cshop/anaconda/
6.	Клиентская ОС Debian 9.4. Официальный сайт https://www.debian.org/index.ru.html
7.	Утилиты Руссиновича https://technet.microsoft.com/ru-ru/library/bb545021.aspx
8.	Анализ защищенности сети Kali Linux 2018.2. https://www.kali.org/
9.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт https://www.openoffice.org/ru/

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

Направление подготовки 01.03.01 Математика
Направленность Преподавание математики и информатики

Рабочая программа дисциплины Информационная безопасность для студентов направленность Преподавание математики и информатики 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 01.03.01 Математика. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Освоивший дисциплину студент 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.

Рабочая программа дисциплины Информационная безопасность для студентов направленность Преподавание математики и информатики 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 Преподавание математики и информатики может быть рекомендована для подготовки студентов направления подготовки 01.03.01 Математика.

Кандидат технических наук,
доцент кафедры наземного транспорта и механики
ФГБОУ ВО «КубГТУ» В.Г. Сутокский

РЕЦЕНЗИЯ

на рабочую программу дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 01.03.01 Математика
Направленность Преподавание математики и информатики

Рабочая программа дисциплины Информационная безопасность для студентов направленность Преподавание математики и информатики 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 01.03.01 Математика. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Содержание рабочей программы 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 задействующие информационно-технологические ресурсы, подлежащие защите; технологии обеспечения информационной безопасности автоматизированных систем.

Рабочая программа дисциплины Информационная безопасность для студентов направленность Преподавание математики и информатики 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 Преподавание математики и информатики может быть рекомендована для подготовки студентов направления подготовки 01.03.01 Математика.

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

В.А. Лазарев