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

УТВЕРЖДАЮ:
Проректор по учебной работе, качеству образования – первый проректор
_____ Хагуров Т.А.
подпись
«29» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.02 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Направление подготовки 01.04.01 Математика

Направленность (профиль) Алгебраические методы защиты информации

Форма обучения Очная

Квалификация Магистр

Краснодар 2020

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

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 № 9 от «10» апреля 2020 г.
Заведующий кафедрой (разработчика) Барсукова В.Ю. _____

Рабочая программа обсуждена на заседании кафедры функционального анализа и алгебры,
протокол № 9 от «10» апреля 2020 г.
Заведующий кафедрой (выпускающей) Барсукова В.Ю. _____

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

Рецензенты:

Сутокский В.Г. к.т.н., доцент кафедры наземного транспорта и механики КубГТУ

Лазарев В.А. д.п.н., 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 «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.06.

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.

Изучение данной учебной дисциплины направлено на формирование у обучающихся общекультурных/общепрофессиональных/профессиональных компетенций (ПК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-1	Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	Основные теоремы алгебры, теории чисел и других разделов теоретической математики	Применять стандартные алгоритмы фундаментальной и прикладной математики	Методами анализа математических Моделей, возникающих в области информационных технологий и защиты информации
2	ПК-4	Способен ориентироваться в современных	О компьютерной реализации	Применять основные математические методы,	использования библиотеки алгоритмов и

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	информационных объектов. Связи компьютерной алгебры и численного анализа.	используемые в анализе типовых алгоритмов.	пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

В результате освоения данной дисциплины обучающийся должен:

Знать:

методологические и технологические основы комплексного обеспечения безопасности АС,

угрозы и методы нарушения безопасности АС,

формальные модели, лежащие в основе систем защиты АС,

стандарты по оценке защищенности АС и их теоретические основы,

методы и средства реализации защищенных АС,

методы и средства верификации и анализа надежности защищенных АС;

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):	**64**	**64**			

Занятия лекционного типа		32	32	-	-	-
Лабораторные занятия		32	32	-	-	-
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:						
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		20	20	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		20	20	-	-	-
Реферат		5	5	-	-	-
Подготовка к текущему контролю		8	8	-	-	-
Контроль:						
Подготовка к экзамену		26,7	26,7			
Общая трудоемкость	**час.**	**144**	**144**	**-**	**-**	**-**
	в том числе контактная работа	**64,3**	**64,3**			
	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.		10		6	13
2	Методология построения систем защищенных АС		8		8	16
3	Политика безопасности.		8		8	14
4	Основные критерии защищенности АС. Классы защищенности АС.		6		10	10
	Итого по дисциплине:		32		32	53

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 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.	Р
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-	Т

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

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

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Подготовка рефератов и научных сообщений	Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.
2	Самостоятельное освоение теории	Рожков А.В. «Перечень электронных источников информации для самостоятельных работ по циклу дисциплин Информационная безопасность магистерской программы АМЗИ и рекомендации по его использованию». Методические указания, утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 г.

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

Для лиц с нарушениями зрения:

– в печатной форме с увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

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

1. Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 10 апреля 2020 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 № 9 от 10 апреля 2020 г.

3. Образовательные технологии.

Активные и интерактивные формы, лекции, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и экзамен. В течение семестра магистры решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый магистр 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, магистру 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 «Теоретические основы компьютерной безопасности» предполагает не только взаимодействия вида «преподаватель - магистр» и «магистр - преподаватель», но и «магистр - магистр». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения магистрами 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 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. Руководящие документы Гостехкомиссии РФ по защите ОС.
10. «Единые критерии» и защита ОС.
11. Основные виды вредоносных программ и методы борьбы с ними.
12. Классификация угроз информации в операционных системах, базах данных, системах электронной почты.
13. Методы обеспечения целостности программно-аппаратной среды. Основные методы защиты памяти.
14. Построение систем защиты с помощью матрицы доступа.

15. Практические методы разработки и реализации политики безопасности.
16. Сравнительный анализ стандартов оценки безопасности компьютерных систем TCSEC, руководящих документов Гостехкомиссии РФ и «Единых критериев». Вредоносный программный код.
17. Классификация вирусов по способу загрузки.
18. Руководящие документы ФСТЭК по защите от вирусов.
19. Сертифицированные антивирусные средства и алгоритмы их работы.
20. Межсетевые экраны. Выбор межсетевого экрана.
21. Настройка служб и администрирование межсетевого экрана.
22. Встраивание межсетевого экрана в систему защиты локальной сети.
23. Требования к защите автоматизированных систем от НСД.
24. Матрица доступа и нормативные акты, регламентирующие ее создание.
25. Выбор и реализация политики сетевой безопасности на предприятии.
26. 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.

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, 2-е изд. [Электронный ресурс]. – СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/133924
2. Нестеров С.А. Основы информационной безопасности, 5-е изд. [Электронный ресурс]. - СПб.: Лань, 2019. - URL: https://e.lanbook.com/reader/book/114688

5.2 Дополнительная литература:

1. Никифоров С.Н. Методы защиты информации. Защита от внешних вторжений, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2019. - URL: https://e.lanbook.com/reader/book/114697
2. Никифоров С.Н. Методы защиты информации. Пароли, скрытие, шифрование, 2- изд. [Электронный ресурс]. - СПб.: Лань, 2019. - URL: https://e.lanbook.com/reader/book/114698/
3. Никифоров С.Н. Методы защиты информации. Шифрование данных, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2019. - URL: https://e.lanbook.com/reader/book/114699/

5.3 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 «Теоретические основы компьютерной безопасности» итоговой формой контроля является экзамен. Для сдачи экзамена 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. В случае затруднений, возникающих у магистров 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:

№ п/п	№ договора	Перечень лицензионного программного обеспечения
1.	Дог. №77-АЭФ/223-ФЗ/2017 от 03.11.2017	DsktpEdu ALNG LicSAPk MVL
2.		VisioPro ALNG LicSAPk MVL
3.		ExchgSvrEnt ALNG LicSAPk MVL
4.		SfBSvr ALNG LicSAPk MVL
5.		SQLSvrEntCore ALNG LicSAPk MVL 2Lic CoreLic
6.		SQLSvrStdCore ALNG LicSAPk MVL 2Lic CoreLic
7.		SysCtrDatactrCore ALNG LicSAPk MVL 2Lic CoreLic
8.		WinSvrDCCore ALNG LicSAPk MVL 2Lic CoreLic
9.		WinSvrSTDCore ALNG LicSAPk MVL 2Lic CoreLic
10.		SysCtrOpsMgrCltML ALNG LicSAPk MVL PerOSE
11.		WinRmtDsktpSrvcsCAL ALNG LicSAPk MVL DvcCAL
12.		VDIStew/MDOP ALNG SubsVL MVL PerDvc
13.	Контракт №79-АЭФ/44-ФЗ/2017 от 16.11.2017	WolframResearch Mathematica Educational Network Premier Service
14.		dotConnect for Oracle Professional Subscription single license
15.		dotConnect for MySQL Professional Subscription single license

16.		dotConnect for PostgreSQL Professional Subscription single license
17.		Navicat Premium v12 (Windows) Non-Commercial ESD 1-4 User License
18.		Design Science MathType Single User English Academic (Windows)
19.	Контракт №69-АЭФ/223-ФЗ от 11.09.2017	Антивирусная защита физических рабочих станций и серверов: Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal License
20.		Антивирусная защита виртуальных серверов: Kaspersky Security для виртуальных сред, Server Russian Edition. 25-49 Virtual Server 1 year Educational Renewal License
21.		Защита почтового сервера от спама: Kaspersky Anti-Spam для Linux Russian Edition. 5000+ MailBox 1 year Educational Renewal License
22.		Антивирусная защита виртуальных рабочих станций (VDI): Kaspersky Security для виртуальных сред, Desktop Russian Edition. 150-249 Virtual Workstation 1 year Educational Renewal License

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
1.	Пакет компьютерной алгебры Sage 9.1. Официальный сайт http://sagemath.org/
2.	Пакет компьютерной алгебры Gap4r11p0. Официальный сайт http://www.gap-system.org/
3.	Пакет компьютерной алгебры PARI/GT 2.13. Официальный сайт http://pari.math.u-bordeaux.fr/
4.	Библиотека для работы с большими целыми числами GMP 6.2.0. 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 10.4. 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 2020.2. https://www.kali.org/
15.	Анализ защищенности сети Snort 3.0. Официальный сайт https://www.snort.org/
16.	Серверная ОС CentOS – 7. Официальный сайт https://www.centos.org/

17.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт https://www.openoffice.org/ru/

8.3 Перечень информационных справочных систем:

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

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

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2.	Семинарские занятия	Не предусмотрены
3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами с предустановленными GAP и Sage
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
7.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

РЕЦЕНЗИЯ

на рабочую программу дисциплины

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

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.

Освоившие программу дисциплины Теоретические основы компьютерной безопасности смогут: Уметь:

проводить анализ автоматизированных систем (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.

Рабочая программа дисциплины Теоретические основы компьютерной безопасности для магистров направленность «Алгебраические методы защиты информации» сочетает теоретическую и практические части. Получение базовых практических сведений и навыков о структуре и алгоритмах символьных математических вычислений.

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.

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

В.А. Лазарев