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.
подпись
«30» июня 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.08 Организационно-правовые методы защиты информации
(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки 01.04.01 Математика
(код и наименование направления подготовки/специальности)

Направленность Алгебраические методы защиты информации
(наименование направленности (профиля) специализации)

Программа подготовки академическая
(академическая /прикладная)

Форма обучения очная
(очная, очно-заочная, заочная)

Квалификация (степень) выпускника магистр
(бакалавр, магистр, специалист)

Краснодар 2017

Рабочая программа дисциплины Организационно-правовые методы защиты информации 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 Организационно-правовые методы защиты информации утверждена на заседании кафедры функционального анализа и алгебры, протокол № _15____ «_9___»__июня_____2017 г

Заведующий кафедрой Барсукова В.Ю. _____

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук,
протокол № __3____ «__20__»__июня_____2017 г.
Председатель УМК факультета Титов Г.Н _____

Рецензенты:

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

Лазарев В.А. д.п.н., зав. кафедрой теории функций КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассматривает задачи информатизации и правовой защиты информации. Изучение этой дисциплины является важной составной частью современного образования в области компьютерных и юридических наук.

1.2 Задачи дисциплины.

Задачи освоения дисциплины «Организационно-правовые методы защиты информации»: раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, а также понятие и виды компьютерных преступлений.

Знания и умения, приобретенные в ходе изучения курса «организационно-правовое обеспечение информационной безопасности» используются обучаемыми при разработке курсовых и дипломных работ.

Задачи дисциплины – дать основы:

- информационного законодательства Российской Федерации;
- системы защиты государственной тайны;
- правил лицензирования и сертификации в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о компьютерных преступлениях.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Организационно-правовые методы защиты информации» относится к вариативной части Блока 1 "Дисциплины (модули)" учебного плана Б1.В.08.

Данная дисциплина как составная часть науки «Информационное право» - правового фундамента информационного общества, 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 (ОК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОК-2	Готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения	содержание основных понятий по правовому обеспечению информационной безопасности; правовые способы защиты	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в
2	ПК-6	способностью к собственному			

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		видению прикладного аспекта в строгих математических формулировках	государственной тайны	правовой информации	области символьных вычислений.

В результате освоения данной дисциплины обучающийся должен:

Знать:

содержание основных понятий по правовому обеспечению информационной безопасности; правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; правила лицензирования и сертификации в области защиты информации; виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

Уметь:

отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.

Владеть:

анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем; навыками работы в нормативно-правовыми актами.

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	-	-	-	-	-
Занятия семинарского типа (семинары, практические занятия)	16	16	-	-	-
	-	-	-	-	-
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		28	28	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		20	20	-	-	-
Реферат		4	4	-	-	-
Подготовка к текущему контролю		8	8	-	-	-
Контроль:						
Подготовка к экзамену		25	25			
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	Законодательство РФ в области информационной безопасности. Правовой режим защиты государственной тайны. Правовые режимы защиты конфиденциальной информации.	36	4	4		28
2	Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Правовое регулирование проведения оперативно-розыскных мероприятий в открытых информационно-телекоммуникационных сетях (ОТКС)	36	4	4		28
3	Концептуальные положения организационного обеспечения информационной безопасности. Принципы организации службы безопасности объекта.	26	4	4		18
4	Подбор сотрудников и работа с кадрами. Организация и обеспечение секретного делопроизводства. Допуск к секретной (конфиденциальной) информации.	19	4	4		11
	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	Законодательство РФ в области информационной безопасности. Правовой режим защиты государственной тайны. Правовые режимы защиты конфиденциальной информации.	Информация как объект правового регулирования. Структура информационной сферы и характеристика ее элементов. Виды информации. Субъекты и объекты правоотношений в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ. Отрасли законодательства, регламентирующие деятельность по защите информации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна. Правовые режимы конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).	Р
2	Лицензирование и сертификация в информационной сфере. Защита интеллектуальной собственности. Правовое регулирование проведения оперативно-розыскных мероприятий в открытых информационно-телекоммуникационных сетях (ОТКС)	Понятия лицензирования по российскому законодательству. Виды деятельности в информационной сфере, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области защиты информации. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации. Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия. Понятие сертификации по российскому законодательству. Понятие интеллектуальной собственности. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем. Защита авторских и смежных прав. Основы патентных правоотношений. Понятие оперативно-розыскной	Э

		деятельности и оперативно-розыскных мероприятий по законодательству РФ. Органы, уполномоченные на осуществление оперативно-розыскной деятельности. Преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Криминалистическая характеристика компьютерных преступлений. Расследование компьютерного преступления. Сбор доказательств. Экспертиза преступлений в области компьютерной информации.	
3	Концептуальные положения организационного обеспечения информационной безопасности. Принципы организации службы безопасности объекта.	Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации. Виды угроз информационной безопасности на объекте защиты и их характеристика. Модели нарушителей информационной безопасности на объекте. Формы преступного посягательства. Оценка ущерба вследствие организационных нарушений информационной безопасности на объекте. Основные направления организационной защиты на объекте. Структура сил и средств организационной защиты информации. Функции, задачи и особенности службы безопасности объекта. Принципы организации службы безопасности объекта. Типовая структура службы безопасности. Основные документы, регламентирующие деятельность службы безопасности объекта. Способы и формы участия сотрудников в организационной защите информации.	Т
4	Подбор сотрудников и работа с кадрами. Организация и обеспечение секретного делопроизводства. Допуск к секретной (конфиденциальной) информации.	Требования к сотрудникам организации, допущенных к секретной (конфиденциальной) информации. Основные критерии приема на работу, связанную с сохранением тайны. Состав документов, необходимых при подборе и приеме сотрудников на работу. Методы проверки кандидатов на должности. Организация обучения персонала, ее методы и формы. Меры по защите информации при увольнении сотрудника. Требования режима секретности при работе с секретными документами. Назначение и задачи секретного делопроизводства. Порядок разработки, учета, хранения, размножения и уничтожения секретных (конфиденциальных) документов. Режим секретности при обработке секретных документов с применением средств вычислительной техники и технических средств иностранного производства. Понятия допуска к	Р

		секретной (конфиденциальной) информации и доступа к секретным (конфиденциальным) работам, документам и изделиям. Номенклатура должностей работников, подлежащих оформлению на допуск. Формы допусков. Оформление, учет и уничтожение справок о допуске. Организация работы по обеспечению контроля за допуском сотрудников организации и ее посетителей.	

2.3.2 Занятия семинарского типа.

Не предусмотрены

1.			
2.			

2.3.3 Практические занятия.

№	Наименование практических работ	Форма текущего контроля
1	3	4
1	Информация как объект правового регулирования. Структура информационной сферы и характеристика ее элементов. Виды информации. Субъекты и объекты правоотношений в области информационной безопасности..	Р
2	Понятие и виды защищаемой информации по законодательству РФ. Отрасли законодательства, регламентирующие деятельность по защите информации	Р
3	Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну.	Э
4	Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция.	Р
5	Понятия лицензирования по российскому законодательству. Виды деятельности в информационной сфере, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области защиты информации.	Р
6	Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации. Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия.	Э
7	Структура сил и средств организационной защиты информации. Функции, задачи и особенности службы безопасности объекта. Принципы организации службы безопасности объекта. Типовая структура службы безопасности.	Р
8	Режим секретности при обработке секретных документов с применением средств вычислительной техники и технических средств иностранного производства. Понятия допуска к секретной	Р

	(конфиденциальной) информации и доступа к секретным (конфиденциальным) работам, документам и изделиям.	

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 лекционных занятий, практических занятий, контрольных работ, тестовых заданий, типовых расчетов, докладов, сдача экзамена.

Вид занятия	Используемые интерактивные образовательные технологии
ЛЗ	Мультимедийная лекция-беседа: «Информация как объект правового регулирования. »
ЛЗ	Дискуссия на тему: «Структура информационной сферы и характеристика ее элементов» с докладами-презентациями
ЛЗ	Круглый стол на тему: «Режим секретности при обработке секретных документов с применением средств вычислительной техники и технических средств иностранного производства.» с докладами-презентациями

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	Количество часов
9	Лекционные занятия	Тема Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации.	2
		Тема Виды угроз информационной безопасности на объекте защиты и их характеристика.	2
		Тема Модели нарушителей информационной безопасности на объекте. Формы преступного посягательства.	2
		Тема Оценка ущерба вследствие организационных нарушений информационной безопасности на объекте.	2
	Практические занятия	Дискуссия на тему: «Основные направления организационной защиты на объекте» с докладами-презентациями	2
		Круглый стол на тему: « Структура сил и средств организационной защиты информации» с докладами-презентациями	2
		Дискуссия на тему: Правовая регламентация лицензионной деятельности в области защиты информации	2
		Компьютерная симуляция: Органы защиты государственной тайны и их компетенция	2
Итого:			8 ч. Лекций, 8 ч. практик

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

Проблемная лекция. Преподаватель в начале и по ходу изложения учебного материала создает проблемные ситуации и вовлекает студентов в их анализ. Разрешая противоречия, заложенные в проблемных ситуациях, обучаемые самостоятельно могут прийти к тем выводам, которые преподаватель должен сообщить в качестве новых знаний.

Лекция-визуализация. В данном типе лекции передача преподавателем информации студентам сопровождается показом различных рисунков, структурно-логических схем,

опорных конспектов, диаграмм и т. п. с помощью ТСО и ЭВМ (слайды, видеозапись, дисплеи, интерактивная доска и т. д.).

Лекция с разбором конкретных ситуаций по форме организации похожа на лекцию-дискуссию, в которой вопросы для обсуждения заменены конкретной ситуацией, предлагаемой обучающимся для анализа в устной или письменной форме. Обсуждение конкретной ситуации может служить прелюдией к дальнейшей традиционной лекции и использоваться для акцентирования внимания аудитории на изучаемом материале.

Дискуссия – это публичное обсуждение или свободный вербальный обмен знаниями, суждениями, идеями или мнениями по поводу какого-либо спорного вопроса, проблемы. Ее существенными чертами являются сочетание взаимодополняющего диалога и обсуждения-спора, столкновение различных точек зрения, позиций.

Компьютерная симуляция – это максимально приближенная к реальности имитация различных процессов (физических, химических, экономических, социальных и проч.) и (или) деятельности с использованием программного обеспечения образовательного назначения.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

Список теоретических вопросов (для подготовки к экзамену)

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.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Список типовых алгоритмов (для самостоятельных занятий)

1. Анализ нарушений безопасности в информационных системах.
2. Обзор Указ Президента РФ. Об утверждении доктрины информационной безопасности Российской Федерации от 05.12.2016 № 486.
3. Указ Президента РФ. О Стратегии национальной безопасности Российской Федерации от 31.12.2015 № 683.
4. Органы, уполномоченные на осуществление оперативно-розыскной деятельности.
5. Преступления в сфере компьютерной информации.
6. Признаки и элементы состава преступления.
7. Криминалистическая характеристика компьютерных преступлений.
8. Анализ Федерального закона. Об электронной подписи от 06.04.2011 №63-ФЗ (ред. от 23.06.2016 N 220-ФЗ).
9. Анализ Закона РФ. О государственной тайне от 21.07.1993 № 5485-1 (ред. от 26.07.2017 N193-ФЗ).
10. Анализ Федерального закона. О персональных данных от 27.07.2006 №152-ФЗ (ред. от 29.07.2017 N 223-ФЗ).
11. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.
12. Правовые режимы конфиденциальной информации: содержание и особенности.
13. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
14. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).
15. Анализ Федерального закона. Об информации, информационных технологиях и о защите информации от 27.07.2006 № 149-ФЗ
16. 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.
17. Анализ Федерального закона. О федеральной службе безопасности от 03.04.1995 №40-ФЗ.
18. Обзор Сборника руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России, 1998 г.

Примерные темы реферативных докладов

1. Работа с нормативно-правовыми документами, регламентирующими вопросы правового регулирования защиты государственной тайны.
2. Изучение порядка осуществления лицензирование и сертификации в области защиты информации.
3. Изучение вопросов защиты интеллектуальной собственности в Российской Федерации.
4. Сравнение полномочия ФСБ и ФСТЭК в области обеспечения информационной безопасности.
5. Состав компьютерных преступлений.

6. Сравнение ФЗ «Об Оперативно-розыскной деятельности» и нормативно-правовых актов и Закона «О частной детективной и охранной деятельности».
7. Разработка должностной инструкции сотрудника подразделения информационной безопасности.

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 «Организационно-правовые методы защиты информации» 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:

№	Перечень лицензионного программного обеспечения
1.	Microsoft office
2.	MS Windows 10 (x64)
3.	MS Office 2013, MS
4.	Office 2010, 7Zip

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.	Практические занятия	аудитория, оснащенная презентационной техникой, учебной мебелью, доской, маркерами и мелом
3.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий, оснащенная учебной мебелью, доской, маркерами и мелом
4.	Текущий контроль, промежуточная аттестация	Аудитория, оснащенная учебной мебелью, доской, маркерами и мелом
5.	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

ОРГАНИЗАЦИОННО ПРАВОВЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки 01.04.01 Математика
Направленность Алгебраические методы защиты информации

Рабочая программа дисциплины Организационно правовые методы защиты информации 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.

Профессионалы в области защиты информации должны ориентироваться в информационном праве. Его изложению и посвящена рабочая программа.

Правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности; понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; правила лицензирования и сертификации в области защиты информации; виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

Рабочая программа дисциплины Организационно правовые методы защиты информации для магистров направленность «Алгебраические методы защиты информации» сочетает теоретическую и практические части, что способствует более глубокому усвоению материала. Считаю, что рабочая программа дисциплины Организационно правовые методы защиты информации 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
ОРГАНИЗАЦИОННО ПРАВОВЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки 01.04.01 Математика
Направленность Алгебраические методы защиты информации

Рабочая программа дисциплины Организационно правовые методы защиты информации 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 Организационно правовые методы защиты информации смогут: отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.

Рабочая программа дисциплины Организационно правовые методы защиты информации 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 Организационно правовые методы защиты информации 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