МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Безопасность распределённых информационных систем государственного и муниципального управления»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация Обеспечение информационной безопасности распределенных информационных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ / Г.А. Остапенко /

Заведующий кафедрой Систем информационной безопасности _____ / А.Г. Остапенко /

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

Цель дисциплины«Безопасность распределенных информационных систем государственного и муниципального управления»- изучение принципов и механизмов обеспечения безопасностираспределенных информационных систем в сфере государственного и муниципального управления.

1.2.Задачиосвоениядисциплины

Для достижения цели ставятся задачи:

- рассмотрение аналитического инструментария для оценки государственных информационных ресурсов и систем
- изучение принципов организации и защиты информационных систем государственного и муниципального управления;
- освоение методологии анализа и синтеза вышеуказанных систем

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Безопасностьраспределённыхинформационныхсистемгосударственногоимуниципальногоуправления»относитсякдисциплинамвариативнойчасти(дисциплинаповыбору)блокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Безопасностьраспределённыхинформационныхсистемгосударственногоимуниципальногоуправления»направленнаформированиеследующихкомпетенций:

ОК-4-способностьюиспользоватьосновыправовыхзнанийвразличныхсферахдеятельности

ПК-5-способностьюпроводитьанализрисковинформационнойбезопасностиавтоматизированнойсистемы

ПК-7-способностьюразрабатыватьнаучно-техническуюдокументацию,готовитьнаучно-техническиеотчеты,обзоры,публикациипорезультатамвыполненныхработ

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ОК-4	знать аспекты нормативно-правовой базы обеспечения информационной безопасности применительно к сфере государственного и муниципального управления.
	уметьиспользовать законодательную и правовую базу в области обеспечения информационной безопасности.
	Владеть навыками работы с универсальными и специализированными пакетами прикладных

	программ для защиты данных.
ПК-5	знатьфизические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем.
	уметьпроводить анализ рисков информационной безопасности автоматизированной системы.
	владетьосновами построения математических моделей текстовой информации и моделей систем передачи информации.
ПК-7	знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих
	уметьформализоватьпоставленнуюзадачу.
	владетьпрофессиональной терминологией в области информационной безопасности

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Безопасностьраспределённыхинформационныхсистемгосударственногоимуниципальногоуправления»составляет13з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всегочасов	Семестры		
		7	8	9
Аудиторныезанятия (всего)	188	54	54	80
В томчисле:				
Лекции	112	36	36	40
Лабораторныеработы (ЛР)	76	18	18	40
Самостоятельнаяработа	244	126	36	82
Курсовойпроект	+			+
Часынаконтроль	36	-	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+	+
Общая трудоемкость: академические часы зач.ед.	 468 13	 180 5	 90 2.5	 198 5.5

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. зан.	СРС	Всего, Час
1	Системы социального управления	Процесс социального управления. Компоненты системы социального управления и их	18	14	36	68

		классификация. Механизмы социального (государственного и муниципального) управления. Основные принципы регионального управления				
2	Особенности управления в РФ на региональном и муниципальном уровнях	Организация муниципального управления в Российской Федерации. Информатизация на региональном уровне: проблемы и перспективы. Информационное обеспечение государственного и муниципального управления с учетом средств информационного обеспечения.	18	14	36	68
3	Государственное и муниципальное управление России и его информационное обеспечение.	Информация в сфере государственного и муниципального управления.Задачи устойчивого развития государственного и муниципального управления в информационной сфере. Общесистемная мотивация ограничения доступа к информации. Информация ограниченного доступа в сфере государственного и муниципального управления	18	12	36	66
4	Безопасность систем распределенной обработки данных	Представление данных в информационных системах. Принципы построения распределенных систем обработки информации. Средства разработки клиентских программ.Серверное программное обеспечение.Технологии построения распределенных информационных систем	14	12	32	58
5	Системы социального управления	Информатизация органов региональной и муниципальной власти. Информационно-аналитическое обеспечение регионального и муниципального управления. Обеспечение безопасности информационных технологий и систем на региональном и муниципальном уровне.	14	6	32	52
6	Специфика распределенных информационных систем в государственном и муниципальном управлении	Системы электронного документооборота. Географические информационные системы. Региональные информационно-аналитические системы. Экспертные системы, системы поддержки принятия решений.	10	6	32	48
7	Концепция обеспечения информационной безопасности электронного правительства	Предоставление государственных услуг с использованием сети Интернет.Единая инфраструктура обеспечения юридически значимого электронного взаимодействия. Защищенная межведомственной система электронного документооборота.Информационные системы планирования и мониторинга деятельности государственных органов. Нормативно-правовая база формирования электронного правительства.	10	6	20	36
8	Информационная безопасность и объекты защиты в компьютерных системах органов государственного и муниципального управления.	Классификация компьютерных систем. Примеры компьютерных системы в сфере государственного и муниципального управления.Угрозы безопасности компьютерных систем в сфере государственного и муниципального управления.Классификация угроз информационной безопасности при использовании компьютерных систем. Способы и каналы несанкционированного доступа к компьютерным системам в сфере государственного и муниципального управления.	10	6	20	36
		Итого	**112**	**76**	**244**	**432**

5.2Перечьлабораторныхработ

1. Построение архитектуры распределенной информационной системы с описанием элементов архитектуры
2. Разработка технического задания по разработке распределенных

информационных систем государственного и муниципального управления

3. Разработка технического задания по модернизации информационной системы
4. Работа с базами данных в различных пакетах прикладных программ
5. Создание функциональной модели информационнойсистемы на базе стандарта IDEF0
6. Оценка прототипов информационных систем с помощью

метода анализа иерархий.

7. Исследование методики решения проблем государственного и муниципального управления при помощи создания распределенных информационных систем
8. Разработка плана и отслеживание процесса создания ивнедрения информационной системы в среде OpenProject.
9. Автоматизированные системы управления технологическими процессами -диспетчерское управление и сбор данных SCADA
10. Электронный документооборот.
11. Информационные системы управления персоналом.
12. Интегрированные информационные системы управления. Стандарты ERP, MRP.
13. Интегрированные информационные системы управления. Стандарты MRP II, CSRP

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплиныпредусматриваетвыполнениекурсовогопроектав9семестредляочнойформыобучения.

Примернаятематикакурсовогопроекта:

1. Системный подход и математические модели в описании технологий и операций информационного терроризма вгосударственном и муниципальном управлении

2. Применение теории катастроф для оценки устойчивости атакуемых нелинейных информационных систем государственного и муниципального управления.

3. Применение теории конфликтов в задачах обеспечения безопасности атакуемых информационных систем государственного и муниципального управления.

4. Применение теории чувствительности для оценки безопасности атакуемых нелинейных информационных систем государственного и муниципального управления.

5. Математические модели интегральной оценки рисков и защищенности атакуемых распределенных информационно-телекоммуникационных систем государственного и муниципального управления.

6. Применение методов сетевого планирования и теории потоков в сетях в задачах обеспечения безопасности атакуемых информационно-телекоммуникационных систем государственного и муниципального управления.

7. Применение теории вероятности и нечетких множеств для интегральной оценки рисков с учетом динамики реализации информационных операций в государственном и муниципальном управлении.

Задачи,решаемыепривыполнениикурсовогопроекта:

•Сформировать знания по теоретическим и методологическим основам по защите информации в области государственного и муниципального управления

• Изучить отечественную и зарубежную нормативную правовую базу по обеспечению безопасности информационных систем.

• Приобрести практический опыт применения математического аппарата, а также использования программ и программных комплексов, реализующих методы анализа информационных рисков.

Курсовойпроектвключатвсебяграфическуючастьирасчетно-пояснительную записку.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениванияикомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ОК-4	знать аспекты нормативно-правовой базы обеспечения информационной безопасности применительно к сфере государственного и муниципального управления.	знание содержания законодательных актов, правовых документов, обеспечивающих защиту информации в сфере государственного и муниципального управления	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь использовать законодательную и правовую базу в области обеспечения информационной безопасности.	умение применять теоретические сведения в правовой области обеспечения безопасности распределенных информационных систем в контексте государственного и муниципального управления	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками	владение навыками	Выполнение работ	Невыполнение

	работы с универсальными и специализированными пакетами прикладных программ для защиты данных.	использования прикладного программного обеспечения защиты данных информационных систем государственного и муниципального управления	в срок, предусмотренный в рабочих программах	работ в срок, предусмотренный в рабочих программах
ПК-5	знать физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем.	знание теоретических основ риск-менеджмента, применимого к распределенным информационным системам государственного и муниципального управления, а также знание основ классифицирования угроз, уязвимостей и факторов, влияющих на безопасность объектов информационной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь проводить анализ рисков информационной безопасности автоматизированной системы.	умение примененять систему показателей для оценки риска принятия управленческих решений руководителем при реализации менеджмента безопасности информационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть основами построения математических моделей текстовой информации и моделей систем передачи информации.	владение навыкамисоставления математические методы и модели для решения прикладных задач оценивания риска с использованием методов теории вероятностей и математической статистики	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-7	знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих	Знание базовых понятий и терминов в сфере обеспечения информационной безопасности, а также государственных и мировых стандартов, принятых в этой области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь формализовать поставленную задачу.	Умение составлять техническую документацию в области обеспечения безопасности информационных ресурсов государственного и муниципального управления использованием теоретических на основе существующей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

		нормативно-правовой базы		
	владеть профессиональной терминологией в области информационной безопасности	Владение навыками практического применения понятийно-терминологической базы в области защиты информационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв7,8,9семестр едляочнойформыобученияподвух/четырехбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
ОК-4	знать аспекты нормативно-правовой базы обеспечения информационной безопасности применительно к сфере государственного и муниципального управления.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь использовать законодательную и правовую базу в области обеспечения информационной безопасности.	Решениестандартныхпрактическихзадач	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
	владеть навыками работы с универсальными и специализированными пакетами прикладных программ для защиты данных.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
ПК-5	знать физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь проводить анализ рисков информационной безопасности автоматизированной системы.	Решениестандартныхпрактическихзадач	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
	владеть основами построения математических моделей текстовой информации и моделей систем передачи информации.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
ПК-7	знать сущность и понятие информации, информационной безопасности и	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%

	характеристику ее составляющих			
	уметь формализовать поставленную задачу.	Решениестандартныхпрактическихзадач	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
	владеть профессиональной терминологией в области информационной безопасности	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОК-4	знать аспекты нормативно-правовой базы обеспечения информационной безопасности применительно к сфере государственного и муниципального управления.	Тест	Выполнение тестана 90-100%	Выполнение тестана 80-90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь использовать законодательную и правовую базу в области обеспечения информационной безопасности.	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
	владеть навыками работы с универсальными и специализированным и пакетами прикладных программ для защиты данных.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
ПК-5	знать физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем.	Тест	Выполнение тестана 90-100%	Выполнение тестана 80-90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь проводить анализ рисков информационной безопасности автоматизированной	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены	Продемонстрирован верный ход решения всех, но не	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

	системы.		верные ответы	получен верный ответ во всех задачах		
	владеть основами построения математических моделей текстовой информации и моделей систем передачи информации.	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
ПК-7	знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих	Тест	Выполнение тестана 90-100%	Выполнение тестана 80-90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	уметь формализовать поставленную задачу.	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
	владеть профессиональной терминологией в области информационной безопасности	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1. Субъектом государственного или муниципального управления является:
а) Соответствующий орган или должностное лицо государства или местного самоуправления;+
б) Руководство предприятий и организаций;
в) Общественные отношения.

2. Объект государственного и муниципального управления – это:
а) Общественные отношения социальных, национальных и иных общностей людей;
б) Поведение общественных объединений, организаций, юридических лиц, поведение отдельных граждан, приобретающее общественное значение;
в) Все вышеперечисленное.+

3. Для чего предназначены информационные системы управления технологическими процессами?

а) для автоматизации функций управленческого персонала.
б) для автоматизации функций производственного персонала.+
в) для автоматизации любых функций компании и охватывают весь цикл работ от проектирования до сбыта продукции
г) для автоматизации работы при создании новой техники или технологии

4. Инструментарий информационной технологии - ...

а) это совокупность данных, сформированная производителем для ее распространения в материальной или в нематериальной форме.
б) это процесс, использующий совокупность средств и методов обработки и передачи данных и первичной информации для получения информации нового качества о состоянии объекта, процесса или явления.
в) это взаимосвязанная совокупность средств, методов и персонала, используемых для обработки данных.
г) это процесс, определяемый совокупностью средств и методов обработки, изготовления, изменения состояния, свойств, формы сырья или материала.
д) это совокупность условий, средств и методов на базе компьютерных систем, предназначенных для создания и использования информационных ресурсов.
е) это совокупность программных продуктов, установленных на компьютере, технология работы в которых позволяет достичь поставленную пользователем цель.+

5. Продолжите предложение: Правовое обеспечение ...

а) подразумевает совокупность математических методов, моделей, алгоритмов и программ для реализации задач информационной системы.
б) включает комплекс технических средств, предназначенных для работы информационной системы.
в) содержит совокупность документов, регулирующих отношения внутри трудового коллектива.
г) содержит в своем составе постановления государственных органов власти, приказы, инструкции министерств, ведомств, организаций, местных органов власти.+
д) определяет всю совокупность данных, которые хранятся в разных источниках.

6. Дополните предложение

Федеральные законы и другие нормативные акты предусматривают разделение информации на категории свободного и _____ доступа.

а) ограниченного+
б) закрытого
в) несанксионированного

7. Ведомственные сети связи –
а) это совокупность технических средств, обеспечивающих передачу и распределение сообщений.
б) это сети электросвязи министерств и иных федеральных органовисполнительной власти, создаваемые для удовлетворения производственных и специальных нуждн, имеющие выход на сеть связи обещего пользования +
в) этокомплексобщегосударственныхиведомственныхавтоматизированны хсистемэлектросвязи,обеспечивающийудовлетворениепотребностейпре дприятий,организацийинаселениястраны

8. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
а) Список стандартов, процедур и политик для разработки программы безопасности
б) Текущая версия ISO 17799
в) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
г) Открытый стандарт, определяющий цели контроля+

9. Что представляет собой стандарт ISO/IEC 27799?
а) Стандарт по защите персональных данных о здоровье+
б) Новая версия BS 17799
в) Определения для новой серии ISO 27000
г) Новая версия NIST 800-60

10.Защита информации от утечки это деятельность по предотвращению:
а) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
б) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
в) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;+
д) несанкционированного доведения защищаемой информации до

неконтролируемого количества получателей информации.

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

1. Особенностями информационного оружия являются:
а) системность
б) открытость
в) универсальность+
г) скрытность+

2. К национальным интересам РФ в информационной сфере относятся:
а) Реализация конституционных прав на доступ к информации+
б) Защита информации, обеспечивающей личную безопасность
в) Защита независимости, суверенитета, государственной и территориальной целостности
г) Политическая экономическая и социальная стабильность
д) Сохранение и оздоровлении окружающей среды

3. К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан …»
а) Информация без ограничения права доступа+
б) Информация с ограниченным доступом
в) Информация, распространение которой наносит вред интересам общества
г) Объект интеллектуальной собственности
д) Иная общедоступная информация

4. Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы
а) Информационные ресурсы
б) Информационная система+
в) Информационная сфера
г) Информационные услуги
д) Информационные продукты

5. Какое определение информации дано в Законе РФ "Об информации, информатизации и защите информации"?
а) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления+
б) Получение сведений из глобальной информационной сети
в) Систематизированные данные об экономике
г) Это результаты компьютерных решений определенных задач

6. Как рассчитать остаточный риск?

а) Угрозы х Риски х Ценность актива
б) (Угрозы х Ценность актива х Уязвимости) х Риски
в) SLE х Частоту = ALE
г) (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля+

7. Что является наилучшим описанием количественного анализа рисков?
а) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
б) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
в) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков+
г) Метод, основанный на суждениях и интуиции

8. Для чего предназначены информационные системы организационного управления?
а) для автоматизации функций управленческого персонала.+
б) для автоматизации любых функций компании и охватывают весь цикл работ от проектирования до сбыта продукции
в) для автоматизации функций производственного персонала.
г) для автоматизации работы при создании новой техники или технологии.
д) Компьютеризированный телефонный справочник является

9. Что можно отнести к инструментарию информационной технологии?
а) электронные таблицы+
б) клавиатурный тренажер
в) системы управления космическим кораблем
г) настольные издательские системы+
д) системы управления базами данных+

10.Продолжите предложение: Техническое обеспечение ...
а) содержит в своем составе постановления государственных органов власти, приказы, инструкции министерств, ведомств, организаций, местных органов власти.
б) содержит совокупность документов, регулирующих отношения внутри трудового коллектива.
в) определяет всю совокупность данных, которые хранятся в разных источниках.
г) подразумевает совокупность математических методов, моделей, алгоритмов и программ для реализации задач информационной системы.
д) включает комплекс технических средств, предназначенных для работы информационной системы.+

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

1. Средства уничтожения, искажения, или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:

а) Информационная война
б) Информационное оружие+
в) Информационное превосходство

2. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:

а) Государственная тайна+
б) Коммерческая тайна
в) Банковская тайна
г) Конфиденциальная информация

3. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:

а) Комплексное обеспечение информационной безопасности
б) Безопасность АС
в) Угрозы информационной безопасности+
г) Атака на автоматизированную систему
д) Политика безопасности

4. Какие угрозы безопасности информации являются непреднамеренными?

а) Взрыв в результате теракта
б) Поджог
в) Забастовка
г) Ошибки персонала+
д) Неумышленное повреждение каналов связи+
е) Некомпетентное использование средств защиты+
ж) Утрата паролей, ключей, пропусков+
з) Хищение носителей информации

5. Что относится к правовым мерам защиты информации?

а) Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения+
б) Действия правоохранительных органов для защиты информационных ресурсов
в) Организационно-административные меры для защиты информационных ресурсов
г) Действия администраторов сети защиты информационных ресурсов

6. Какие правовые документы решают вопросы информационной

безопасности?

а) Уголовный кодекс РФ+
б) Конституция РФ+
в) Закон "Об информации, информатизации и защите информации"+
г) Закон РФ "О государственной тайне"+
д) Закон РФ "О коммерческой тайне"+
е) Закон РФ "О лицензировании отдельных видов деятельности"+
ж) Закон РФ "Об образовании"
з) Закон РФ " Об электронной цифровой подписи "+

7. Что такое идентификация?

а) Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации+
б) Указание на правильность выполненных операций по защите информации
в) Определение файлов, которые изменены в информационной системе несанкционированно
г) Выполнение процедуры засекречивания файлов
д) Процесс периодического копирования информации

8. Заключительным этапом построения системы защиты является:

а) сопровождение +
б) планирование
в) анализ уязвимых мест

9. Классификация информационных систем по способу организации не включает в себя один из перечисленных пунктов:

а) Системы на основе архитектуры файл – сервер;
б) Системы на основе архитектуры клиент – сервер;
в) Системы на основе многоуровневой архитектуры;
г) Системы на основе интернет/интранет – технологий;
д) Корпоративные информационные системы.+

10. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.

а) Комплексное обеспечение информационной безопасности
б) Безопасность АС
в) Угроза информационной безопасности
г) Атака на автоматизированную систему+
д) Политика безопасности

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

1. Социум и основы социального управления.
2. Специфика социальной организации. Классы, виды и формы управления социумом.

3. Процесс социального управления. Компоненты системы социального управления.
4. Механизмы социального (государственного и муниципального) управления.
5. Принципы социального управления.
6. Основы государственного и муниципального управления. Системы социального управления.
7. Специфика социального управления в Российской Федерации на региональном и муниципальном уровнях.
8. Основные проблемы информатизации на региональном уровне
9. Информация в сфере государственного и муниципального управления. Государственное и муниципальное управление России и его информационное обеспечение.
10. Триединая задача устойчивого развития государственного и муниципального управления в информационной сфере.
11. Ограничения доступа к информации в системах государственного и муниципального управления.
12. Информация ограниченного доступа в сфере государственного и муниципального управления.
13. Сущность информационных систем и технологий государственного и муниципального управления.
14. Этапы создания автоматизированных систем информационного обеспечения.
15. Единое информационное пространство. Проблемы информационного обеспечения систем государственного и муниципального управления.
16. Концептуальная модель безопасности информационной системы
17. Закон №149-ФЗ «Об информации информационных технологиях и защите информации». Основные требования. Область действия
18. Классификация информации. Особенности доступа к информации различной категории доступа
19. Информация как объект правовых отношений. Виды информации доступ, к которой не может быть ограничен
20. Ценность информации. Подходы к оценке ценности информации в контексте государственного и муниципального управления
21. Конфиденциальная информация. Информация ограниченного доступа. Виды конфиденциальной информации.
22. Требования к защите информационных систем обработки данных в сфере государственного и муниципального управления
23. Права и обязанности обладателя информации в соответствии с Законом

№ 149-ФЗ

24. Угрозы информационной безопасности. Алгоритм определения актуальных угроз безопасности персональных данных?
25. Списки уязвимостей ПО. Количественно-качественные характеристики угроз информационной безопасности.
26. Модель угроз информационной безопасности. Модель злоумышленника.
27. Базы данных. Специфика БД в контексте государственного и муниципального управления
28. Принципы построения систем обработки информации.
29. Технологии построения распределенных информационных систем
30. Составляющие риска информационной безопасности. Управление рисками информационной безопасности в сфере государственного и муниципального управления.
31. Законодательство РФ в области информационной безопасности. Законы и нормативно-методические документы
32. Проблемы обеспечения информационной безопасности при организации информационного взаимодействия муниципальных учреждений

7.2.5 Примерныйпереченьзаданийдлярешенияприкладныхзадач

1. Виды систем государственного управления.
2. Функции информационной системы государственного и муниципального управления
3. Характеристика распределенной обработки данных
4. Базовые технологии обработки запросов в архитектурах файл-сервера и клиент-сервера
5. Структурная схема методики построения топологических моделей информационных операций.
6. Риск информационной безопасности. Виды риска. Методы оценки риска
7. Задачи обеспечение безопасности информации на государственном уровне.
8. Государственная политика РФ в области информационной безопасности
9. Модели защиты информации. Модели компьютерной безопасности и их классификация.
10. Подсистемы и средства защиты данных в распределенных информационных системах
11. Требования к системам обнаружения вторжений и антивирусным средствам

12. Профиль защиты. Понятие аудита информационной безопасности. 44. Виды и задачи аудита информационных систем в государственном и муниципальном управлении
13. Классификация методов аудита. Активный аудит. Аудит на основе профиля защиты

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

Зачет/Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Системы социального управления	ОК-4, ПК-5, ПК-7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Особенности управления в РФ на региональном и муниципальном уровнях	ОК-4, ПК-5, ПК-7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Государственное и муниципальное управление России и его информационное обеспечение.	ОК-4, ПК-5, ПК-7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Безопасность систем распределенной обработки данных	ОК-4, ПК-5, ПК-7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Системы социального управления	ОК-4, ПК-5, ПК-7	Тест, контрольная работа, защита

			лабораторных работ, защита реферата, требования к курсовому проекту….
6	Специфика распределенных информационных систем в государственном и муниципальном управлении	ОК-4, ПК-5, ПК-7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
7	Концепция обеспечения информационной безопасности электронного правительства	ОК-4, ПК-5, ПК-7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
8	Информационная безопасность и объекты защиты в компьютерных системах органов государственного и муниципального управления.	ОК-4, ПК-5, ПК-7	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором,ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампрактикосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымвметодическихматериалах.Примерноевремязащитынаодногостудентасоставляет20мин.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основнаялитература:

1. Методическое обеспечение оценки и регулирования рисков распределенных информационных систем : Учеб. пособие / Г. А. Остапенко [и др.]. - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2011. - 178 с. - 182-77; 250 экз.

2. Язов Ю.К. Проектирование защищенных информационно-телекоммуникационных систем [Электронный ресурс] : Учеб. пособие / Ю. К. Язов. - Электрон. текстовые, граф. дан. (6,97 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.

3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебно-методическое пособие / П.Н. Девянин. — Москва : Горячая линия-Телеком, 2012. — 320 с. — ISBN 978-5-9912-0147-6. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/5150.

Дополнительнаялитература:

1. Методические указания к самостоятельным работам по дисциплинам «Информационная безопасность телекоммуникационных систем», «Информационная безопасность распределенных информационных систем» для студентов специальностей 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. Ю. К. Язов. - Электрон. текстовые, граф. дан. (379 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

2. Основы построения систем обнаружения вторжений [Электронный ресурс] : Методические указания к практическим занятиям по дисциплине «Информационная безопасность распределенных информационных систем» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения / Каф. систем информационной безопасности; Сост. Е. А. Москалева. - Электрон. текстовые, граф. дан. (619 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

3. Методические указания к курсовому проектированию по дисциплине "Информационная безопасность РИС" для студентов специальности 090303 "Информационная безопасность автоматизированных систем" очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост. Е. А. Москалева. - Электрон. текстовые, граф. дан. (407 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.

8.2Перечеьинформационныхтехнологий,используемыхприосуществлениобразовательногопроцессаподисциплине,включаяпереченьлице

нзионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой, а так же учебная аудитория для проведения занятий лабораторного типа.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Безопасностьраспределённыхинформационныхсистемгосударственногоимуниципальногоуправления»читаютсялекции,проводятсялабораторныеработы,выполняетсякурсовойпроект.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Методикавыполнениякурсовогопроектаизложенавучебно-методическомпособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременноивустановленныесроки.

Контрольусвоенияматериаладисциплиныпроизводитсяпроверкойкурсовогопроекта,защитойкурсовогопроекта.

Видучебныхзанятий	Деятельностьстудента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.

Лабораторнаяработа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельнаяработа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточнойаттестации.
Подготовка к промежуточнойаттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.