МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Проректор по научной работе
(наименование должности полностью)
О.Г. Добросердов
(подпись, инициалы, фамилия)
«28» 06 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Системы документооборотаи средства защиты циркулирующей в них информации
(наименование дисциплины)

направление подготовки 10.06.01
шифр согласно ФГОС ВО

Информационная безопасность
наименование направления подготовки

Методы и системы защиты информации, информационная безопасность
наименование профиля (специализация подготовки)

квалификация (степень) выпускника: Исследователь. Преподаватель-исследователь

форма обучения очная
(очная, заочная)

Курск – 2016

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (уровень подготовки кадров высшего образования)направления подготовки10.06.01 «Информационная безопасность», на основании учебного плана профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 11 «27» 06 2016 г.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения аспирантов по направлению подготовки 10.06.01 «Информационная безопасность», профиля (специализации) «Методы и системы защиты информации, информационная безопасность» на заседании кафедры информационной безопасности, протокол № 1 от «30» 08 2016 г.

Зав. кафедрой _____ М.О. Таныгин

Разработчик программы _____ Ю.А. Халин

Согласовано:

Директор научной библиотеки _____ В.Г. Макаровская

Начальник отдела аспирантуры и докторантуры _____ О.Ю. Прусова

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность»профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 5 «30» 08 2017 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол 1 от 28.08.2017

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 9 «26» 03 2018 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол 12 от 29.06.2018.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 9 «24» 06 2019 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол 11 от 27.06.2019

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №11 «29» 06 2020г. на заседании кафедры информационной безопасности.

Зав. кафедрой ______ / протокол N 1 от 31.08.2020

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №8 «31» 05 2021г. на заседании кафедры информационной безопасности.

Зав. кафедрой ______ / протокол N 11 от 28.06.2021

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №__ «__»________20__г. на заседании кафедры информационной безопасности.

Зав. кафедрой____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №__ «__»________20__г. на заседании кафедры информационной безопасности.

Зав. кафедрой____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №__ «__»________20__г. на заседании кафедры информационной безопасности.

Зав. кафедрой____

1 Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения ОП

1.1 Цель преподавания дисциплины

Целью преподавания дисциплины является формирование представления об электронном документе как новой сущности в правовых отношениях, предоставление аспирантам систематизированного подхода к проблеме использования систем электронного документооборота (ЭДО) и информационных систем (ИС). Курс знакомит аспирантов с проблемами и методологией информационной безопасности систем документооборота и направлен на приобретение обучающимися глубоких и всесторонних знаний по современным методам анализа, исследования и разработки методов и средств защиты в области электронногодокументооборота с обеспечением юридической значимости обрабатываемой информации.

1.2 Задачи изучения дисциплины

Задачами освоения дисциплины являются:

– изучить методологию исследовательской деятельности, основные проблемы в области информационной безопасности электронных документов;

– изучить основные положения и методы разработки систем документооборота;

– выполнить разработку целей, задач и методов научного исследования по тематике дисциплины;

– выполнить практические работы по настройке и использованию средств обеспечения безопасности распределенного электронного документооборота;

– приобрести навыки использования организационных форм и методов научных исследований впри проектировании системы документооборота организации;

– приобрести навыки критического анализа и оценки уровня защищенности систем электронного документооборота;

– приобрести навыки реализации процессов управления информационной безопасностью, направленных на эффективное управление информационной безопасностью конкретной организации.

1.3 Компетенции, формируемые в результате освоения дисциплины

У обучающихся формируются следующие **компетенции**:

ОПК-1 – способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность;

ОПК-2 – способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для

решения конкретных исследовательских задач в области обеспечения информационной безопасности;

ОПК-3 – способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;

ПК-3 – способность анализировать степень защищенности и совершенствовать системы документооборота и средства защиты циркулирующей в них информации;

ПК-4 – способность разрабатывать новые и совершенствовать имеющиеся методы, аппаратно-программные и организационные средства защиты информационных систем и ресурсов.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Системы документооборота и средства защиты циркулирующей в них информации» (Б1.В.ДВ.1) находится в вариативной части базового блока УП, изучается на 3 курсе, в 5 семестре.

3 Содержание и объем дисциплины

3.1 Содержание дисциплины и лекционных занятий

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единицы (з.е.), 108 часов

Таблица 3.1 –Объём дисциплины по видам учебных занятий

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	
в том числе:	36,1
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
экзамен	не предусмотрено
зачет	0,1
Аудиторная работа (всего):	36
в том числе:	
лекции	18
лабораторные занятия	не предусмотрено
практические занятия	18
Самостоятельная работа обучающихся (всего)	72
Контроль/экз (подготовка к экзамену)	не предусмотрено

Таблица 3.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел, темы дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*	Компетенции
		лек., час	лаб., час	пр., час			
1	2	3	4	5	6	7	8
1	Введение в курс «Системы документооборота и средства защиты циркулирующей в них информации»	1, 2 часа	0	1, 2 часа	У-1, У-2, У-4	С 1-2 недели	ОПК-1, ОПК-3
2	Аудит информационной безопасности СЭД. Методы и средства защиты информации в СЭД.	2, 4 часа	0	2, 4 часа	У-1, У-2, У-3, У-6	С 3-6 недели	ОПК-1, ОПК-2, ОПК-3, ПК-3
3	Технические средства защиты информации в СЭД. Организационные средства защиты информации. Законодательные средства защиты информации.	3, 4 часа	0	3, 4 часа	У-1, У-2, У-3, У-6, МУ-1, МУ-2	КО 7-10 недели	ОПК-3, ПК-3, ПК-4
4	Система защиты электронного документооборота организации. Организация работы с персоналом по обеспечению защиты информации в СЭД.	4, 2 часа	0	4, 2 часа	У-2, У-3, У-5, У-7, МУ-1, МУ-2	КО 11-12 недели	ОПК-1, ОПК-2, ОПК-3, ПК-3
5	Развитие международного законодательства в области защиты информации и информационной безопасности.	5, 2 часа	0	5, 2 часа	У-2, У-3, У-5, У-7, МУ-4	КО 13-14 недели	ОПК-1, ОПК-2, ОПК-3, ПК-3
6	Удостоверяющие центры. Порядок выдачи и использования ключей электронной подписи.	6, 4 часа	0	6, 4 часа	У-1, У-2, У-3, У-6, МУ-3, МУ-4	К 15-18 недели	ОПК-3, ПК-3, ПК-4
7	ИТОГО	18		18		З	

Э– экзамен, КР – курсовая работа; КП – курсовой проект, К – контрольная работа, З – зачет, С – собеседование, СР – семестровая работа, Кл – коллоквиум, КО – контрольный опрос, МК – автоматизированный программированный контроль (машинный контроль).

Таблица 3.3 – Краткое содержание лекционного курса

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Введение в курс«Системы документооборота и средства защиты циркулирующей в них информации»	Общая характеристика электронного документооборота. Основные понятия и определения. Цели внедрения электронного документооборота.
2	Аудит информационной безопасности СЭД. Методы и средства защиты информации в СЭД.	Аудит информационной безопасности – общие понятия. Общие требования по защите информации в ЛВС. Защита информации при работе с системами управления базами данных. Идентификация и аутентификация пользователей в системе электронного документооборота.
3	Технические средства защиты информации в СЭД. Организационные средства защиты информации. Законодательные средства защиты информации.	Защита информации от НСД в компьютерных системах. Программно-аппаратные комплексы защиты информации, криптографические средства защиты информации. Регламент информационной безопасности предприятия. Законодательство в области защиты информации: ФЗ «О государственной тайне», ФЗ «О коммерческой тайне», ФЗ «О персональных данных», ФЗ «Об электронной подписи».
4	Система защиты электронного документооборота организации. Организация работы с персоналом по обеспечению защиты информации в СЭД.	Типовая структура системы электронного документооборота организации. Встроенные механизмы обеспечения безопасности в системах электронного документооборота. Трудности внедрения СЭД на предприятии. Юридическая и техническая грамотность персонала организации при работе с СЭД.
5	Развитие международного законодательства в области защиты информации и информационной безопасности.	Международные нормативно-правовые акты и сотрудничество государств в сфере информационной безопасности. Защита персональных данных за рубежом.
6	Удостоверяющие центры. Порядок выдачи и использования ключей электронной подписи.	Виды электронной подписи. Аккредитованные удостоверяющие центры: требования, функциональность, обязательства и ответственность при компрометации ключей электронной подписи (ЭП). Порядок выдачи ключа электронной подписи. Состав сертификата ЭП. Применение электронной подписи в системах электронного документооборота.

3.2 Лабораторные работы и (или) практические занятия
3.2.2 Практические занятия

Таблица 3.5 –Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Семинар на тему «Механизмы обеспечения информационной безопасности электронных документов»	2
2	Семинар на тему «Защищенные системы электронного документооборота»	2
3	Семинар на тему «Применение электронной подписи в системах электронного документооборота»	2
4	Практическое занятие «Первичное развертывание сети ViPNet»	2
5	Практическое занятие «Настройка межсетевого взаимодействия»	4
6	Практическое занятие «ViPNet Деловая почта»	2
7	Практическое занятие «Формирование ключей электронной подписи»	4
Итого		18

3.3 Самостоятельная работа аспирантов (СРС)

Таблица 3.6 – Самостоятельная работа студентов

№	Наименование раздела дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1	Механизмы обеспечения информационной безопасности электронных документов Подготовка *доклада* и выступление с ним на практическом занятии	2 - 3 неделя	5
2	Защищенные системы электронного документооборота Подготовка *доклада с презентацией* и выступление с ним на практическом занятии	4 - 5 неделя	5
3	Применение электронной подписи в системах электронного документооборота Подготовка *доклада с презентацией* и выступление с ним на практическом занятии	6 - 7 неделя	5
4	Углубленное изучение программно-аппаратных средств обеспечения информационной безопасности электронного документооборота	8 - 16 неделя	35
5	Написание *материалов для выступления на научно-технической конференции с публикацией материалов в сборниках, включенных в РИНЦ.*		17
6	Развитие международного законодательства в области защиты информации и информационной безопасности	17 - 18 неделя	15

	Подготовка реферата в рамках предложенной тематикиТемы реферата – см. Приложение А.		
Итого			72

Общие рекомендации аспирантам изложены в Методических указаниях к выполнению самостоятельной работы.

4 Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

Аспиранты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки:

– методических рекомендаций, пособий по организации самостоятельной

– работы студентов;

– тем рефератов;

– вопросов к зачету;

– методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

– удовлетворение потребности в тиражировании научной, учебной и методической литературы.

5 Образовательные технологии

В соответствии с требованиями Федеральным государственным образовательным стандартом высшего образования направления подготовки *10.06.01 – «Информационная безопасность»,* утвержденного Министерством образования и науки Российской Федерации приказом № 301 от 05.04.2017г., реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков аспирантов.В рамках дисциплины предусмотрены встречи с экспертами и специалистами по информационной системам.

Таблица 5.1 – Образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объем, час.
1	Семинар на тему «Механизмы обеспечения информационной безопасности электронных документов»	Разбор конкретных ситуаций	2
2	Семинар на тему «Защищенные системы электронного документооборота»	Разбор конкретных ситуаций	2
3	Семинар на тему «Примение электронной подписи в системах электронного документооборота»	Компьютерная симуляция	2
4	Практическое занятие «Настройка межсетевого взаимодействия»	Разбор конкретных ситуаций	2
5	Практическое занятие «ViPNet Деловая почта»	Разбор конкретных ситуаций	2
Итого			10

6 Фонд оценочных средств для проведения промежуточной аттестации

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 6.1 Этапы формирования компетенции

Код компетенции, содержание компетенции	Дисциплины (модули) при изучении которых формируется данная компетенция
1	2
ОПК-1 – способность формулировать научные задачи в области обеспечения информационной безопасности, применять для	Б1.В.ОД.4Методология научных исследований при подготовке диссертации Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6Методы и системы защиты информации,

их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	информационная безопасность Б1.В.ДВ.1.1Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ОПК-2 – способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1Подготовка к сдаче и сдача государственного экзамена Б4.Д.1Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ОПК-3 –способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1Подготовка к сдаче и сдача государственного экзамена Б4.Д.1Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ПК-3 – способность анализировать степень защищенности и совершенствовать системы документооборота и средства	Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел

защиты циркулирующей в них информации	как средство реализации асимметричного шифрования Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ПК-4 – способность разрабатывать новые и совершенствовать имеющиеся методы, аппаратно-программные и организационные средства защиты информационных систем и ресурсов	Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)

Средствами промежуточного контроля успеваемости студентов являются защита практических заданий, опросы на практических занятиях по темам лекций. В конце семестра – зачет. Перечень вопросов к зачеты представлен в приложении Б.

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 6.2 Показатели и критерии определения уровня сформированности компетенций (частей компетенций)

№ п/п	Код компетенции (или её части)	Уровни сформированности компетенции		
		Пороговый (удовлетворительный)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
1	ОПК–1 – способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных	Знать: -методологию исследовательской деятельности, основные проблемы в области информационной безопасности; Уметь: - определять программу проведения исследований,	Знать: - основы культуры научного исследования в информационной безопасности, Уметь: - использовать и применять их в современных информационно-коммуникационных технологиях	Знать: - основные положения и методы социальных, гуманитарных и экономических наук при решении педагогических задач Уметь: - использовать теоретический материал в

	исследований, внедрять полученные результаты в практическую деятельность.	Владеть: - планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач	Владеть: - способностью к критическому анализу результатов научного творчества	педагогической, научно-исследовательской, творческой, управленческой деятельностях Владеть: -организационными формами и методами проведения научных исследований;
2	ОПК–2 – способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.	Знать: -методологию исследовательской деятельности, основные проблемы в области информационной безопасности; Уметь: - определять ее цель, задачи, разрабатывать гипотезу и определять способы ее проверки, Владеть: - планированием исследовательской деятельности и определением целесообразных методов для решения поставленных в исследовании задач	Знать: - основы культуры научного исследования, Уметь: - использовать и применять их в современных информационно-коммуникационных технологиях Владеть: - способностью к критическому анализу и оценке современных научных достижений	Знать: - основные положения и методы социальных, гуманитарных и экономических наук при решении педагогических задач Уметь: - использовать теоретический материал в педагогической, научно-исследовательской, творческой, управленческой деятельностях Владеть: -организационными формами и методами проведения научных исследований;
3	ОПК–3 – способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности.	Знать: -стандарты в области информационной безопасности; Уметь: - сопоставлять характеристики объекта информатизации действующим стандартам, Владеть: - комплексной оценки защищённости	Знать: - методологические подходы применения нормативных документов приоценки защищённости объектов информатизации, Уметь: - выявлять недекларируемые угрозы объекту информатизации	Знать: - принципы формирования комплексных отчётов по аудиту информационной безопасности Уметь: - вырабатывать методические рекомендации по реализации систем защиты Владеть: -организационными

		объекта информатизации	Владеть: - способностью к критическому анализу используемых методов аудита информационной безопасности	формами и методами проведения научных исследований;
4	ПК–3 – способность анализировать степень защищённости и совершенствовать системы документооборота и средства защиты циркулирующей в ней информации	Знать: -стандарты в области информационной безопасности системы документооборота; Уметь: - сопоставлять характеристики систем документооборота действующим стандартам, Владеть: - комплексной оценки защищённости систем документооборота	Знать: - методологические подходы применения нормативных документов при оценке защищённости систем документооборота, Уметь: - выявлять недекларируемые угрозы систем документооборота Владеть: - способностью к критическому анализу используемых методов аудита информационной безопасности	Знать: - принципы формирования комплексных отчётов по аудиту информационной безопасности систем документооборота Уметь: - вырабатывать методические рекомендации по формированию политик безопасности в системах документооборота Владеть: -организационными формами и методами проведения научных исследований;
5	ПК–4 – способность разрабатывать новые и совершенствовать имеющиеся методы аппаратно-программные и организационные средства защиты информационных систем и ресурсов.	Знать: -стандарты в отношении технических и аппаратно-программных средств защиты информации ; Уметь: - сопоставлять характеристики аппаратно-программных средств защиты информации действующим стандартам, Владеть: - комплексной оценки защищённости	Знать: - методологические подходы применения нормативных документов при оценке качества технических и аппаратно-программных средств защиты информации, Уметь: - выявлять недекларируемые угрозы систем и подбирать для них адекватные технических и	Знать: - принципы формирования комплексных отчётов по аудиту технических и аппаратно-программных средств защиты информации Уметь: - вырабатывать методические рекомендации по формированию политик безопасности Владеть: -организационными

		аппаратно-программных средств защиты информации	аппаратно-программных средств защиты информации Владеть: - способностью к критическому анализу используемых методов аудита информационной безопасности	формами и методами проведения научных исследований;

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 6.3 Паспорт комплекта оценочных средств

№ п/п	Раздел (тема) дисциплины	Код компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№№ заданий	
1	2	3	4	5	6	7
1	Введение в курс«Системы документооборота и средства защиты циркулирующей в них информации»	ОПК-1	Лекция Практическое занятие	Лекция с элементами проблемного изложения	См. МУ	Оценивая ответ, члены комиссии учитывают следующие *основные критерии*: – уровень теоретических знаний (подразумевается не только формальное воспроизведение информации, но и понимание предмета, которое подтверждается правильными ответами на дополнительные, уточняющие вопросы, заданные членами комиссии); – умение использовать теоретические знания при анализе конкретных проблем, ситуаций; –качество изложения материала, то есть обоснованность, четкость,
		ОПК-3	Лекция Практическое занятие	Собеседование	См. МУ	
2	Аудит информационной безопасности СЭД. Методы и средства защиты информации в СЭД	ОПК-1, ОПК-2,	Лекция	Лекция с элементами проблемного изложения	См. МУ	
		ОПК-3, ПК-3	Практическое занятие	Практическая работа	См. МУ	

						логичность ответа, а также его полнота (то есть содержательность, не исключающая сжатости);
3	Технические средства защиты информации в СЭД. Организационные средства защиты информации. Законодательные средства защиты информации	ОПК-1, ОПК-2,	Лекция Практическое занятие	Сообщение студента	См. МУ	- способность устанавливать внутри- и межпредметные связи, оригинальность и красота мышления, знакомство с дополнительной литературой и множество других факторов.
		ОПК-3, ПК-3, ПК-4	Лекция Практическое занятие	Практическая работа		*Критерии оценок:*
4	Система защиты электронного документооборота организации. Организация работы с персоналом по обеспечению защиты информации в СЭД	ОПК-1, ОПК-2	Лекция Практическое занятие	Сообщение студента Практическая работа	См. МУ	Оценка *зачтено* – исчерпывающее владение программным материалом, понимание сущности рассматриваемых процессов и явлений, твѐрдое знание основных положений дисциплины, умение применять концептуальный аппарат при анализе актуальных проблем. Логически последовательные, содержательные, конкретные ответы на все вопросы экзаменационного билета и на дополнительные вопросы членов комиссии, свободное владение источниками. Предложенные в качестве самостоятельной работы формы работы (примерный план исследовательской деятельности; пробная рабочая программа) приняты без замечаний.
		ОПК-3, ПК-3, ПК-4	Лекция Практическое занятие			
5	Развитие международного законодательства в области защиты информации и информационной безопасности	ОПК-1, ОПК-2, ОПК-3	Лекция Практическое занятие	Сообщение студента	См. МУ	
6	Удостоверяющие центры. Порядок выдачи и использования ключей электронной подписи	ОПК-1, ОПК-2	Лекция Практическое занятие	Сообщение студента	См. МУ	Оценка *не зачтено* – отсутствие ответа хотя бы на один из основных вопросов, либо грубые ошибки в ответах, полное непонимание смысла проблем, не достаточно полное владение терминологией. Отсутствие выполненных самостоятельных дополнительных работ.
		ОПК-3, ПК-3, ПК-4	Лекция Практическое занятие	Практическая работа		

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Список методических указаний, используемых в образовательном процессе, представлен в п. 7.2;
- Оценочные средства представлены в учебно-методическом комплексе дисциплины.

Далее приведены типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Описание правил оформления результатов оценивания

Подготовлен и отправлен файл экспорта – 1 балл.

Создан межсетевой мастер-ключ – 1 балл.

Импортированы данные– 3 балла.

Созданы ключевые наборы – 1 балл.

Прекращена сетевое взаимодействие – 2 балла.

ЗАДАНИЕ № 1

Согласно методическим указаниям к проведению практического занятия по дисциплине «Системы документооборота и средства защиты циркулирующей в них информации»:Настройка межсетевого взаимодействия: / Юго-Зап. гос. ун-т; сост.: И.В. Калуцкий, С.В. Пономарев. Курск, 2014. 20 с.: ил. 15,.Библиогр.: с. 20: изучена методика настройки взаимодействия между сетями ViPNet. Так же содержит подробное описание и порядок создания файлов экспорта, ключевой информации и правила создания межсетевых ключей.

Предмет(ы) оценивания	Объект(ы) оценивания (заполняется при оценивании компетенций)	Показатели и критерии оценки
Использование теоретических знаний и практических навыков в профессиональной деятельности	Деятельность предприятия (организации) – места прохождения учебной (производственной) практики	Показатели знать основные направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности, оценивать затраты и риски, формировать стратегию создания систем информационной безопасности в соответствии со стратегией развития организации. Критерии Описаны проблемы межпроцессорного взаимодействия и взаимоблокировки процессов. Изучены файловые системы и механизмы их защиты. Умение проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты. Проанализированы фундаментальные и прикладные проблемы информационной безопасности.

Условия выполнения задания

1. Место (время) выполнения задания (*на учебной/ производственной практике, на рабочем месте, например, в цеху организации (предприятия), мастерской ОУ (ресурсного центра), организации, предприятия, на полигоне, в учебной фирме, учебной аудитории и т.п.):* учебная аудитория
2. Максимальное время выполнения задания: 180 мин.
3. Вы можете воспользоваться *(указать используемое оборудование (инвентарь), расходные материалы, литературу и другие источники, информационно-коммуникационные технологии и проч.*):

1. Настройка межсетевого взаимодействия: Методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И.В. Калуцкий, С.В. Пономарев. Курск, 2014. 20 с.: ил. 15,.Библиогр.: с. 20

ЗАДАНИЕ № 2

Текст задания:

Согласно методическим указаниям к проведению практического занятия по дисциплине «Системы документооборота и средства защиты циркулирующей в них информации»: ViPNet деловая почта: / Юго-Зап. гос. ун-т; сост.: И.В. Калуцкий, С.В. Понома-рèв Курск, 2012. 20 с.: ил. 10. Библиогр.: с. 20: Содержат сведения по вопросам настройке и использовании ПО ViPNet Деловая почта.

Предмет(ы) оценивания	Объект(ы) оценивания (заполняется при оценивании компетенций)	Показатели и критерии оценки
Использование теоретических знаний и практических навыков в профессиональной деятельности	Деятельность предприятия (организации) – места прохождения учебной (производственной) практики	Показатели Умеет организовывать защищенную передачу электронных документов по открытым каналам связи по всему маршруту следования документа от отправителя к получателю в сетиViPNet. Критерии Создано правило автопроцессинга для обработки файлов. Указан произвольный каталог и выставлена маска файлов для docx файлов. Создано правило автопроцессинга для входящих писем. Создать письмо с подписью пользователя и отправить всем пользователям сети, отправлено вложение с подписью пользователю в сети.

Условия выполнения задания

1. Место (время) выполнения задания (*на учебной/ производственной практике, на рабочем месте, например, в цеху организации (предприятия), мастерской ОУ (ресурсного центра), организации, предприятия, на полигоне, в учебной фирме, учебной аудитории и т.п.):* учебная аудитория
2. Максимальное время выполнения задания: 6час.
3. Вы можете воспользоваться *(указать используемое оборудование (инвентарь), расходные материалы, литературу и другие источники, информационно-коммуникационные технологии и проч.*):

1. ViPNet Деловая почта: Методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И.В. Калуцкий, С.В. Пономарèв Курск, 2012. 20 с.: ил. 10. Библиогр.: с. 20

Типовая настройка межсетевого взаимодействия

Порядок выполнения работы

Подготовка и отправка файла экспорта

После настройки сети VIPNet необходимо сделать так, чтобы они могли обмениваться информацией между собой, т.е. объеди-нить их. Для этого, нам необходимо создать файлы в ЦУС1 с опи-санием нашей сети, ее структурой и т.д. и передать это всѐ в ЦУС2 с помощью защищенного носителя информации.

Открываем ЦУС1 и находим вкладку: Службы-Экспорт… и нажимаем Enter и оказываемся в меню экспорта: нажимаем на вкладку добавить и появляется окно с предложением назначить номер сети и ее имя.

После добавления сети, нам необходимо указать все ТК и уз-лы, которые имеются в данной сети. Можно это сделать или через вкладку Узлы или через вкладку ТК. Однако необходимо добавить ВСЕ узлы и коллективы, которые необходимо связать с другой сетью. В противном случае - другая сеть их не увидит и как следствие взаимодействие будет нарушено.

Настройка через вкладку Узлы:

Добавить необходимо все АП с помощью вкладки добавить. После их добавление, необходимо указать ТК, для этого щелкаем по вкладке ТК и выбираем имеющийся ТК.

Настройка через вкладку ТК осуществляется в обратномпо-рядке: сначала выбирается ТК, а потом добавляются узлы.

После настройки данной сети необходимо указать СМ-шлюз, через который данная сеть будет осуществлять обмен с другой се-тью. Для этого щелкаем по вкладке СМ-шлюз и выбираем его из списка.

Далее, необходимо скопировать данные на съемный защи-щенный носитель информации и передать в ЦУС2.Для этого, необ-ходимо нажать на вкладку Копировать и подтвердить копирование в директорию по умолчанию(C:\Program Files\InfoTeCS\ViPNetAdministrator\NCC\NEW\EXPORT).Обязательным условием успешного формирования файла для экспорта является наличие в сети машины с ПО VIPNetCoordinator.Так же необ-ходимо заново сформировать все справочники для сети. После это-го, в данной папке создается папка с именем сети, которую необхо-димо скопировать на защищенный съемный носитель и перенести в ЦУС2.

Создание межсетевого мастер-ключа

Теперь необходимо сгенерировать межсетевой мастер-ключ, необходимый для взаимодействия сетей. Для этого в УКЦ выбира-ем папку Ключевой центр / Доверенные сети ViPNet / Мастер-ключи / Текущие.

Далее нужно создать общий межсетевой ключ. Для этого нуж-но щелкнуть правой кнопкой мыши и выбрать пункт создать и вы-брать универсальный.

После этого необходимо установить пароль, затем щелкнуть правой кнопкой мыши и выбрать пункт Экспорт.

Ключ сохранится в папке КС\EXPORT.Его нужно скопиро-вать вместе с информацией для экспорта и передать в другую сеть.

Импорт данных

Теперь приступаем к объединению двух сетей. Для этого, нам необходимо скопировать содержимое папки (ИМЕННО СОДЕР-ЖИМОЕ ПАПКИ,А НЕ

САМУ ПАПКУ С СОДЕРЖИМЫМ!) в папку C:\Program Files\InfoTeCS\ViPNetAdministrator\NCC\ IMPORT\NEW.

После этого, запускаем ЦУС2 и ждем, когда появится сообще-ниеоб необработанном импорте.

После появления данного сообщение выбираем да и оказыва-емся в меню необработанного импорта ,где нам необходимо вы-брать вкладку Обработать всѐ и ждать окончания обработки.

После этого появится сообщение о необходимости перена-строить сеть. Так же, нам необходимо связать типы коллективов. Начнем с настройки сети. Выбираем пункт Службы/Адресная ад-министрация-Структура сети VIPNet. Далее выбираем вкладку Межсетевые каналы, где нам необходимо указать СМ-шлюз для нашей сети, для чего достаточно нажать клавишу Enter и выбрать предложенный сервер.

После этого, необходимо вернуться в меню и выбрать пункт Выдать таблицы маршрутизации. Настройка окончена, теперь пе-реходим к регистрации типов коллективов. Выбираем пункт Служ-бы/Прикладная администрация-регистрация типов коллективов. Там мы увидим, что теперь у нас появилось 2 коллектива, и нам необходимо их связать между собой. Для этого нажимаем на вклад-ку Связи/Добавить и выбираем предложенный коллектив из табли-цы.

После этого получаем два объединенных коллективов. Настройка окончена, но нам необходимо заново сформировать все справочники, в виду новой конфигурации сети, для этого выбираем вкладку Службы/Сформировать все справочники и ждѐмоконча-ния.

Так же необходимо поместить межсетевой ключ в папку KC\IMPORT,затем выбрать межсетевые ключи-входящие щелкнуть правой кнопкой мыши и нажать импорт. Затем нужно применить данный ключ. Для этого так же щелкаем правой кнопкой мыши и выбираем пункт - ввести в действие.

Таким образом мы настроили ЦУС2 и теперь тоже самое нам необходимо сделать и для ЦУС1.

Создание ключевых наборов

После настройки ЦУСов необходимо зайти в УКЦ и принять сертификаты администраторов и обновить ключевуюинформа-цию. Для этого выбираем пункт меню Сервис / Автоматически со-здать / Ключевые наборы. Затем переходим Ключевой центр / Своя сеть ViPNet / Ключи / Ключевые наборы , щелкаем правой кнопкой мыши и выбираем пункт Перенести в ЦУС. Затем в ЦУСевыбира-ем Управление/отправка и отсылаем данные.После этого межсете-вое взаимодействие настроено.

Прекращение сетевого взаимодействия

Для прекращения сетевого взаимодействия между сетями необходимо зайти в Службы/Экспорт и удалить файл экспорта. После этого межсетевое взаимодействие прекратиться. Затем необ-ходимо зайти в Службы/Адресная администрация-структура сети VIPNet и сформировать новые таблицы маршрутизации.

Рейтинговый контроль не предусмотрен.

Описание оценочных средств и шкал оценивания ответов см. в Таблице 6.3.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная и дополнительная литература

а) Основная литература:

1. Калуцкий, И. В. Программно-аппаратные средства защиты информационных систем [Текст] : учебное пособие / И. В. Калуцкий, А. Г. Спеваков ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2014. – 179, [2] с.

2. Ярочкин, В. И. Аудит безопасности фирмы: теория и практика [Электронный ресурс] : учебное пособие / В. И. Ярочкин, Я. Бузанова. - Москва : Академический Проект ; Парадигма, 2012. - 352 с. – Режим доступа : Biblioclub.ru

3. Экономическая безопасность [Текст] : учебное пособие / [В. А. Богомолов [и др.] ; под ред. В. А. Богомолова. - 2-е изд., перераб. и доп. - Москва : ЮНИТИ, 2014. - 295 с.

б) Дополнительная литература:

1. Радченко, Г. И. Распределенные вычислительные системы [Электронный ресурс] : учебное пособие / Г. И. Радченко. - Челябинск: Фотохудожник, 2012. - 184 с. Режим доступа : http://window.edu.ru/resource/646/76646

2. Ветров, Ю. В. Криптографические методы защиты информации в телекоммуникационных системах [Электронный ресурс] : учебное пособие / Ю. В. Ветров, С. Б. Макаров. - СПб.: Изд-во Политехн. ун-та, 2011. - 174 с. – Режим доступа : http://window.edu.ru/resource/170/75170

3. Проскурин, В. Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах [Текст] : учебное пособие для студ. вуз. / С. В. Крутов, И. В. Мацкевич. - М.: Радио и связь, 2000. - 168 с.

4. Зегжда, Д. П. Способы безопасности информационных систем [Текст] : учеб. пособие для студ. вуз. / А. М. Ивашко. – М. : Горячая линия – Телеком, 2000. – 452 с.

5. Жуков, И. Ю. Стохастические методы и средства защиты информации в компьютерных системах и сетях [Текст] / под ред. И. Ю. Жукова. - М. : КУДИЦ-ПРЕСС, 2009. - 512 с.

6. Романов, О. А. Организационное обеспечение информационной безопасности [Текст] : учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с.

7. Семкин, С. Н. Основы организационного обеспечения информационной безопасности объектов информатизации [Текст] : учебное пособие / С. Н. Семкин [и др.]. - М. : Гелиос АРВ, 2005. - 192 с.

8. Тихонов, В. А. Информационная безопасность : концептуальные, правовые, организационные и технические аспекты [Текст] : учебное пособие / В. А. Тихонов, В. В. Райх. - М. : Гелиос АРВ, 2006. – 528 с.

7.2 Перечень методических указаний

1. Первичное развертывание сети ViPNet [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И. В. Калуцкий, С. В. Пономарёв. - Курск, 2014. - 26 с.
2. Действия при изменениях в структуре сети ViPNet [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И. В. Калуцкий, С. В. Пономарёв. - Курск, 2014. - 26 с.
3. Настройка межсетевого взаимодействия [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И. В. Калуцкий, С. В. Пономарёв. - Курск, 2014. - 20 с.
4. ViPNet Деловая почта [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И. В. Калуцкий, С. В. Пономарёв. - Курск, 2012. - 20 с.

7.3 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Корпорация Microsoft [официальный сайт]. Режим доступа: http://www.microsoft.com/
2. Рускоязычный сайт сообщества Ubuntu [сайт]. Режим доступа: http://ubuntu.ru/

7.4 Перечень информационных технологий

1. MicrosoftOfficePowerPoint;
2. MicrosoftOfficeExcel;
3. ДиспетчеррисунковMicrosoftOffice:
4. MATLAB.

7.5 Другие учебно-методические материалы

Программно-аппаратный комплекс защиты информации «SECRETNET 5.0»/ Методические указаний по выполнению лабораторной работы. Состав. В.Н. Лопин, М.О. Таныгин, КГТУ, Курск, 2008.

Базы данных, информационно-справочные и поисковые системы:

1. www.edu.ru - федеральный портал «Российское образование»
2. www.elibrary.ru/defaultx.asp - научная электронная библиотека.

8 Материально-техническое обеспечение дисциплины

Для обеспечения учебного процесса используются: лекционная аудитория, оснащенная мультимедийными средствами, аудитория для практических занятий, компьютерная аудитория, обеспечивающая выход в ИНТЕРНЕТ.

8 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

№ изменения	Номера страниц				Всего	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1		4			1	01.09.17	Приказ ФГБОУ «Юго-Западный государственный университет» № 576 от 31.08.2017 г. « О внесении изменений в приказ №263 от 29.03.2017 г. « Об утверждении норм времени для расчета учебной и других видов работы»
2		9			1	01.09.17	Приказ № 301 от 05.04.2017 г.
3		21-22			2	13.12.17	Протокол заседания кафедры ИСиТ №10 от 13.12.17

Приложение А

Темы рефератов

1. Актуальные проблемы науки XXI века.
2. Античная философия - основа европейской научной рациональности.
3. Взаимосвязь науки, общества, производства.
4. Естественные и гуманитарные науки: особенности методологических и методических принципов.
5. Естественные науки в Древнем Мире.
6. Задачи и возможности эмпирического исследования.
7. Закон как ключевой элемент научной теории
8. Индукция, дедукция и абдукция.
9. Интуиция и логика в искусстве и науке.
10. Историография науки
11. Исторический анализ: сущность и основное содержание метода.
12. История естествознания. Естественные науки как продукт исторического развития.
13. История информатики. Информатика как продукт исторического развития.
14. История науки и методологии.
15. История социальных наук. Социальные науки как продукт исторического развития.
16. Картезианская революция в естествознании.
17. Кибернетический подход к управлению в живых организмах, машинах и обществе.
18. Классификация наук.
19. Классический механицизм.
20. Кризис механицизма конца 19 - начала 20 века.
21. Математические модели в естественных науках.
22. Методологическая роль моделей в естественных науках.
23. Методологическая роль моделей в социальных науках.
24. Методологические принципы в естественных науках.
25. Методы обоснования научной теории.
26. Модели и моделирование в познании.
27. Наука в XIX-XX веках.
28. Наука в XVII - XVIII веках.
29. Наука в эпоху средневековья.
30. Наука как объект методологического анализа.
31. Наука, паранаука и псевдонаука.
32. Научное знание как система, его особенности и структура.
33. Научное наблюдение.
34. Научные факты и способы их установления, обобщения
35. Общенаучные категории и синтез современного научного знания.
36. Общенаучные методы исследования. Методологическое единство науки.
37. Понятие метода научного познания. Классификация методов научного познания.

38. Проблема «начала» науки.
39. Проблема периодизации истории науки.
40. Проблема, гипотеза, теория, закон как формы научного знания.
41. Развитие научного знания в Индии и Китаи.
42. Развитие научного знания на Ближнем Востоке.
43. Развитие эволюционных представлений в естественных науках.
44. Синергетический подход как методология познания саморазвивающихся объектов.
45. Системный подход в исследовании социальных систем.
46. Системный подход в исследовании социальных систем.
47. Системный подход как методология познания целостных объектов.
48. Сущность экстремальных принципов и их роль в формализме естественных наук
49. Формализация и математизация.
50. Эволюционные теории.
51. Экспериментальные методы естествознания.
52. Эпоха Возрождения - начало современной науки.

Методические указания к написанию реферата см. в: История и философия науки: методические указания к выполнению самостоятельной работы аспирантов/ Юго-Зап. гос. ун-т; сост.: И.А. Асеева. Курск, 2015. 17 с.: ил. 3. Библиогр.: с. 17.

Приложение Б
Перечень вопросов к зачету

1. Основные понятия документооборота: виды представления информации, документы, документопотоки, документооборот и другие основные понятия.
2. Экономическая система: структура, потоки информации, функции управления.
3. Жизненный цикл документов.
4. Понятие электронного документооборота, его особенности.
5. Отличия российского документооборота от зарубежного.
6. Экономическая информационная система и СЭД как ее часть.
7. Безбумажная технология управления.
8. Понятие электронного документа. Виды, особенности. Представление документов в СЭД.
9. Концепция электронного документооборота. Принципы СЭД. Основные требования к функциональности СЭД.
10. Автоматизация составления электронных документов. Автоматизация процесса ввода потоков входных документов. Перевод документов из бумажной формы в электронную и наоборот.
11. Контроль версий в СЭД.
12. Электронная подпись.
13. Классификация методов защиты информации В СЭД
14. Организационные методы защиты электронного документооборота.
15. Программные средства защиты информации в СЭД.
16. Аппаратные средства защиты информации в СЭД.
17. Архитектуры и способы построения СЭД.
18. Разграничение доступа пользователей в СЭД.
19. Современное законодательство и нормативно-методическое регулирование электронного документооборота.
20. Зарубежное законодательство в области электронного документооборота и обеспечения его безопасности.
21. Международное сотрудничество в области защиты электронного документооборота.
22. Типичные угрозы безопасности электронного документооборота.
23. Встроенные механизмы обеспечения информационной безопасности в системах электронного документооборота.
24. Известные преступления в сфере электронного документооборота.
25. Перспективы и тенденции развития средств и методов защиты информации в системах электронного документооборота