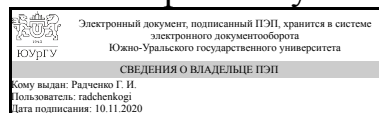


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и
компьютерных наук



Г. И. Радченко

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.35 Угрозы информационной безопасности автоматизированных систем

для специальности 10.05.03 Информационная безопасность автоматизированных систем

уровень специалист тип программы Специалитет

специализация Информационная безопасность автоматизированных систем

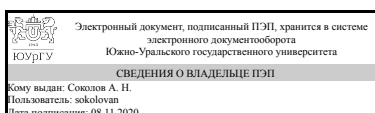
критически важных объектов

форма обучения очная

кафедра-разработчик Защита информации

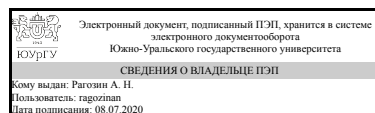
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
к.техн.н., доцент



А. Н. Рагозин

1. Цели и задачи дисциплины

Дисциплина "Угрозы информационной безопасности автоматизированных систем" имеет целью изучение основных типов угроз информационной безопасности, характерных для современных авто-матизированных систем (АС) в защищенном исполнении, а также основных подходов к проведению количественного и качественного анализа информационных рисков. Задачами дисциплины являются: - приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в области анализа угроз информационной безопасности АС, оцен-ки рисков информационных ресурсов предприятия; - формирование у обучаемых целостного представления об управлении информационными рис-ками.

Краткое содержание дисциплины

Тема 1. Введение Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные поня-тия и определения. Понятие угрозы информационной безопасности. Тема 2. Перечисление угроз информационной безопасности Классификация угроз информационной безопасности. Основные категории угроз. Систем-ный подход к перечислению угроз информационной безопасности. Нормативная база. Подход «Общих критериив». Методики STRIDE и DREAD. Тема 3. Модели угроз и модели нарушителя Понятие модели угроз и модели нарушителя. Типовое содержание моделей угроз и моделей нарушителя. Отечественная и зарубежная нормативная база. Нормативные требования ФСТЭК России и ФСБ России в части формирования моделей угроз и моделей нарушителя. Тема 4. Анализ рисков и управление рисками Понятие анализа рисков. Количественный и качественный анализ рисков. Нормативная база: отечественные и зарубежные методологии и рекомендации. Особенности анализа рисков в АС кредитно-финансовых учреждений. Нечеткие модели методы анализа информационных рисков.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-3 способностью проводить анализ защищенности автоматизированных систем	Знать:категории угроз информационной безопасности в автоматизированных системах
	Уметь:определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; формулировать и оценивать угрозы информационной безопасности в автоматизированных системах; оценивать информационные риски в автоматизированных системах
	Владеть:навыками формирования перечня угроз информационной безопасности в АС; методами количественной и качественной оценки

	информационных рисков;
ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Знать:сущность и понятие информации, информационной безопасности , угроз , рисков
	Уметь:анализировать и обобщать информацию
	Владеть:профессиональной терминологией в области информационной безопасности
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать:основные категории угроз информационной безопасности в автоматизированных системах основные модели угроз и модели нарушителя в автоматизированных системах
	Уметь:определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; формулировать и оценивать угрозы информационной безопасности в автоматизированных системах
	Владеть:навыками формирования перечня угроз информационной безопасности в АС
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Знать:место анализа рисков в общей системе обеспечения информационной безопасности
	Уметь:оценивать информационные риски в автоматизированных системах
	Владеть:методами количественной и качественной оценки информационных рисков
ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Знать:основные методы построения систем защиты от угроз нарушения конфиденциальности, целостности и доступности информации
	Уметь:анализировать решения , компоненты автоматизированных систем с целью выявления потенциальных уязвимостей ИБ
	Владеть:навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.17 Основы информационной безопасности, Б.1.26 Управление информационной безопасностью, Б.1.30.01 Разработка защищенных автоматизированных систем	В.1.09 Обеспечение информационной безопасности на критически важных объектах

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
------------	------------

Б.1.17 Основы информационной безопасности	Знать сущность и понятие ИБ и характеристику ее составляющих, источники и классификацию угроз ИБ, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности;
Б.1.30.01 Разработка защищенных автоматизированных систем	Знать основные методы построения систем защиты от угроз нарушения конфиденциальности, целостности и доступности информации; уметь формулировать общие требования к подсистеме защиты информации, применять основные методы; владеть навыками использования современных оценочных стандартов в области информационной безопасности. Знать общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем; уметь формировать требования к подсистемам информационной безопасности автоматизированных систем различных типов.
Б.1.26 Управление информационной безопасностью	Знать научные основы, цели, принципы, методы и технологии управленческой деятельности; уметь работать в коллективе, принимать управленческие решения и оценивать их эффективность; владеть навыками выбора, обоснования, реализации и контроля результатов управленческого решения;

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		9
Общая трудоёмкость дисциплины	108	108
<i>Аудиторные занятия:</i>	48	48
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	24	24
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	60	60
Подготовка к практическим занятиям	30	30
Подготовка к зачёту	10	10
Подготовка рефератов	20	20
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение	12	6	6	0
2	Перечисление угроз информационной безопасности	12	6	6	0
3	Модели угроз и модели нарушителя	12	6	6	0
4	Анализ рисков и управление рисками	12	6	6	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Понятие угрозы информационной безопасности.	6
2	2	Классификация угроз информационной безопасности. Основные категории угроз. Системный подход к перечислению угроз информационной безопасности. Нормативная база. Подход «Общих критериев». Методики STRIDE и DREAD.	6
3	3	Понятие модели угроз и модели нарушителя. Типовое содержание моделей угроз и моделей нарушителя. Отечественная и зарубежная нормативная база. Нормативные требования ФСТЭК России и ФСБ России в части формирования моделей угроз и моделей нарушителя.	6
4	4	Понятие анализа рисков. Количественный и качественный анализ рисков. Нормативная база: отечественные и зарубежные методологии и рекомендации. Особенности анализа рисков в АС кредитно-финансовых учреждений. Нечеткие модели методы анализа информационных рисков.	6

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Анализ автоматизированных систем. Понятие и анализ угроз информационной безопасности автоматизированных систем.	6
2	2	Основы системного анализа. Классификация угроз информационной безопасности автоматизированных систем с использованием системного анализа. Нормативная база. Подход «Общих критериев». Методики STRIDE и DREAD.	6
3	3	Системный анализ и построение модели угроз и модели нарушителя. Типовое содержание моделей угроз и моделей нарушителя. Отечественная и зарубежная нормативная база. Нормативные требования ФСТЭК России и ФСБ России в части формирования моделей угроз и моделей нарушителя.	6
4	4	Понятие анализа рисков. Методики оценки рисков. Количественный и качественный анализ рисков. Нормативная база: отечественные и зарубежные методологии и рекомендации. Нечеткие модели методы анализа информационных рисков. Построение экспертных систем оценки рисков с использованием нечеткой логики.	6

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Подготовка к практическим занятиям	<p>1. Котенко И.В., Котухов М.М., Марков А.С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информаци-онно-вычислительных сетей. - СПб.: ВУС, 2000. - 320 с. 2. Тихонов В.А., Райх В.В. Информационная безопасность: организационные, правовые и технические аспекты. М.: Гелиос АРВ, 2006. 516 с. 3. Цирлов В.Л. Основы информационной безопасности: краткий курс. - Ростов н/Д: Феникс, 2008. - 254 с. 4. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. - Киев: МК-Пресс, 2006. - 320 с. 5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: ИЦ «Академия», 2008. 332 с. 6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994. - Кн. 1. - 400 с. 7. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. - М.: Энергоатомиздат, 1994. - Кн. 2. - 176 с. 8. Пикфорд Д. Управление рисками. - М.: ООО «Вершина», 2004. - 352 с. 9. Птускин А.С. Нечеткие модели и методы в менеджменте. - М.: Издательство МГТУ им. Н.Э. Баумана, 2008. - 216 с. 10. Курило А.П., Зефилов С.Л., Голованов В.Б. и др. Аудит информационной безопасности. М.: Издательская группа «БДЦ пресс», 2006. 304 с. 11. Правовое обеспечение информационной безопасности. / Учебник под общ. науч. ред. В. А. Минаева и др. М.: Маросейка, 2008. 368 с.</p>	30
Подготовка к зачёту	<p>1. Котенко И.В., Котухов М.М., Марков А.С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности</p>	10

	<p>автоматизированных систем и информаци-онно-вычислительных сетей. - СПб.: ВУС, 2000. - 320 с. 2. Тихонов В.А., Райх В.В. Информационная безопасность: организационные, правовые и технические аспекты. М.: Гелиос АРВ, 2006. 516 с. 3. Цирлов В.Л. Основы информационной безопасности: краткий курс. - Ростов н/Д: Феникс, 2008. - 254 с. 4. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. - Киев: МК-Пресс, 2006. - 320 с. 5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: ИЦ «Академия», 2008. 332 с. 6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994. - Кн. 1. - 400 с. 7. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. - М.: Энергоатомиздат, 1994. - Кн. 2. - 176 с. 6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994. - Кн. 1. - 400 с. 7. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. - М.: Энергоатомиздат, 1994. - Кн. 2. - 176 с. 8. Пикфорд Д. Управление рисками. - М.: ООО «Вершина», 2004. - 352 с. 9. Птускин А.С. Нечеткие модели и методы в менеджменте. - М.: Издательство МГТУ им. Н.Э. Баумана, 2008. - 216 с. 10. Курило А.П., Зефилов С.Л., Голованов В.Б. и др. Аудит информационной безопасности. М.: Издательская группа «БДЦ пресс», 2006. 304 с. 11. Правовое обеспечение информационной безопасности. / Учебник под общ. науч. ред. В. А. Минаева и др. М.: Маросейка, 2008. 368 с.</p>	
Подготовка рефератов	<p>1. Котенко И.В., Котухов М.М., Марков А.С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информаци-онно-вычислительных сетей. - СПб.: ВУС, 2000. - 320 с. 2. Тихонов В.А., Райх В.В. Информационная безопасность: организационные, правовые и технические аспекты. М.:</p>	20

	<p>Гелиос АРВ, 2006. 516 с. 3. Цирлов В.Л. Основы информационной безопасности: краткий курс. - Ростов н/Д: Феникс, 2008. - 254 с. 4. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. - Киев: МК-Пресс, 2006. - 320 с. 5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: ИЦ «Академия», 2008. 332 с. 6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994. - Кн. 1. - 400 с. 7. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. - М.: Энергоатомиздат, 1994. - Кн. 2. - 176 с. 8. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994. - Кн. 1. - 400 с. 9. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. - М.: Энергоатомиздат, 1994. - Кн. 2. - 176 с. 10. Пикфорд Д. Управление рисками. - М.: ООО «Вершина», 2004. - 352 с. 11. Птускин А.С. Нечеткие модели и методы в менеджменте. - М.: Издательство МГТУ им. Н.Э. Баумана, 2008. - 216 с. 12. Курило А.П., Зефирова С.Л., Голованов В.Б. и др. Аудит информационной безопасности. М.: Издательская группа «БДЦ пресс», 2006. 304 с. 13. Правовое обеспечение информационной безопасности. / Учебник под общ. науч. ред. В. А. Минаева и др. М.: Маросейка, 2008. 368 с.</p>	
--	---	--

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Использование информационных ресурсов и баз данных	Практические занятия и семинары	Построение экспертных систем с использованием нечёткой логики в MATLAB matlab.exponenta.ru http://matlab.exponenta.ru/index.php	14
Использование методов, основанных на изучении практики (case studies)	Практические занятия и семинары	Решение практических задач	10

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
Разбор конкретных ситуаций	Работа в малых группах

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ОПК-5 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Контрольные вопросы и задания для проведения текущего контроля	№№ 1-6
Все разделы	ПК-3 способностью проводить анализ защищенности автоматизированных систем	Контрольные вопросы и задания для проведения текущего контроля	№№ 7-15
Все разделы	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Контрольные вопросы и задания для проведения текущего контроля	№№ 1-8
Все разделы	ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Контрольные вопросы и задания для проведения текущего контроля	№№ 1-11
Все разделы	ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Зачёт	№№ 1-21

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Контрольные вопросы и задания для проведения текущего контроля	Ответы на вопросы	Зачтено: Ответ на один вопрос Не зачтено: Ответ на ноль вопросов
Контрольные вопросы и задания для проведения текущего контроля	Ответы на вопросы	Зачтено: Ответ на один вопрос Не зачтено: Ответ на ноль вопросов
Контрольные вопросы и задания для проведения текущего контроля	Ответ на вопросы	Зачтено: Ответ на один вопрос

		Не зачтено: Ответ на ноль вопросов
Контрольные вопросы и задания для проведения текущего контроля	Ответы на вопросы	Зачтено: Ответ на один вопрос Не зачтено: Ответ на ноль вопросов
Зачёт	Ответы на вопросы	Зачтено: Ответ на один вопрос Не зачтено: Ответ на ноль вопросов

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Контрольные вопросы и задания для проведения текущего контроля	<ol style="list-style-type: none"> 1. Основные понятия в области риск-менеджмента: угроза, уязвимость, атака, риск, оценка риска. Их взаимосвязь. 2. Место анализа рисков в общей схеме управления ИБ 3. Количественный подход к оценке рисков. Достоинства, недостатки подхода. 4. Качественный подход к оценке рисков. Достоинства, недостатки подхода. 5. Экономическая модель оценки рисков. 6. Вероятностная модель оценки рисков.
Контрольные вопросы и задания для проведения текущего контроля	<ol style="list-style-type: none"> 7. ГОСТ Р ИСО 31000-2010: принципы и схема процесса риск менеджмента. 8. Управление рисками и жизненный цикл информационной системы. 9. ГОСТ Р ИСО/МЭК 15408-1-2012 «Общие критерии оценки безопасности информационных технологий. Введение и общая модель». Основные понятия и их взаимосвязь. 10. ГОСТ Р ИСО/МЭК 15408-1-2012 «Общие критерии оценки безопасности информационных технологий. Введение и общая модель». Профиль защиты 11. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Схема процесса менеджмента рисков. Модель PDCA. 12. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Этап «Установление контекста менеджмента риска». 13. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Этап «Идентификация риска» 14. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Этап «Оценка риска» 15. ISO/IEC 27005:2011 «Менеджмент рисков информационной безопасности». Обработка риска. Мониторинг и пересмотр, передача и принятие риска.
Контрольные вопросы и задания для проведения текущего контроля	<ol style="list-style-type: none"> 1 Классификация угроз информационной безопасности. 2 Основные категории угроз. 3 Системный подход к перечислению угроз информационной безопасности. Нормативная база. Подход «Общих критериев». 4 Модели угроз и модели нарушителя 5 Понятие модели угроз и модели нарушителя. Типовое содержание моделей угроз и моделей нарушителя. Отечественная и зарубежная нормативная база. Нормативные требования ФСТЭК России и ФСБ России в части формирования моделей угроз и моделей нарушителя. 6 Анализ рисков и управление рисками 7 Понятие анализа рисков. Количественный и качественный анализ рисков. Нормативная база: отечественные и зарубежные методологии и

	<p>рекомендации.</p> <p>8 Нечеткие модели методы анализа информационных рисков.</p>
Контрольные вопросы и задания для проведения текущего контроля	<ol style="list-style-type: none"> 1. Модель риска типа «узла»: основное содержание, пример. 2. Вероятностная модель: основное содержание, достоинства, недостатки. 3. Отличие вероятностной модели оценки рисков от экономической модели оценки рисков. 4. Понятие профиля риска для бизнеса. 5. Концепция «эшелонированной защиты». 6. Понятие уровня безопасности организации. 7. Этапы оценки рисков. 8. Актив, типы активов. 9. Риск, угроза, уязвимость, механизмы контроля. 10. Процесс управления рисками информационной безопасности, основные этапы. 11. Понятие уровня зрелости организации с точки зрения управления рисками безопасности.
Зачёт	<ol style="list-style-type: none"> 1 Область применения процесса определения угроз безопасности информации 2 Идентификация источников угроз и угроз безопасности информации 3 Оценка вероятности (возможности) реализации угроз безопасности информации и степени возможного ущерба 4 Мониторинг и переоценка угроз безопасности информации 5 Типы нарушителей 6 Виды и потенциал нарушителей 7 Возможные способы реализации угроз безопасности информации 8 Оценка вероятности (возможности) реализации угрозы безопасности информации 9 Оценка степени возможного ущерба от реализации угрозы безопасности информации 10 Определение актуальности угрозы безопасности информации 11 Формирование экспертной группы 12 Проведение экспертной оценки 13 Определение показателя «затрачиваемое время» 14 Определение показателя «техническая компетентность нарушителя» 15 Определение показателя «знание нарушителем проекта и информационной системы» 16 Определение показателя «возможности нарушителя по доступу к информационной системе» 17 Определение показателя «оснащенность нарушителя» 18. Экономическая модель оценки риска: основное содержание, достоинства, недостатки. 19 Понятие профиля риска для бизнеса. 20. Концепция «эшелонированной защиты». 21. Понятие уровня безопасности организации.

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. БДИ: Безопасность. Достоверность. Информация рос. журн. о безопасности бизнеса и личности ООО "Журн. "БДИ" журнал. - М., 2006-2015
2. Анискин, Л. Г. Аварийность и безопасность [Текст] Л. Г. Анискин ; под ред. А. К. Васильева. - М.: Б. И., 2006. - 63 с. ил.

3. Хашковский, А. В. Автоматизированное рабочее место инженера службы охраны труда Учеб. пособие Юж.-Урал. гос. ун-т, Каф. Безопасность жизнедеятельности; ЮУрГУ. - Челябинск: Издательство ЮУрГУ, 1999. - 82,[1] с. ил.
4. Гловацкая, А. П. Методы и алгоритмы вычислительной математики Учеб. пособие по специальностям "Сети связи и системы коммутации", "Радиосвязь, радиовещание и телевидение", "Средства связи с подвижными объектами", "Ав. техника". - М.: Радио и связь, 1999. - 407,[1] с. ил.
5. Долинин, В. П. Электрические системы и сети Учеб. пособие по лаб. работам для студентов спец. 1004 ЧГТУ, Каф. Системы электроснабжения; В. П. Долинин, В. Я. Боос, В. И. Стасяк; ЮУрГУ. - Челябинск: Издательство ЧГТУ, 1996. - 39,[1] с.
6. Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы [Текст] учеб. для вузов по направлению 552800 "Информатика и вычисл. техника" и по специальностям 220100 "Вычисл. машины, комплексы, системы и сети", 220200 "Автоматизир. системы обработки информ. и упр.", 220400 "Програм. обеспечение вычисл. техники и автоматизир. систем" В. Г. Олифер, Н. А. Олифер. - 3-е изд. - СПб. и др.: Питер, 2007. - 957 с. ил.
7. Пятибратов, А. П. Вычислительные системы, сети и телекоммуникации Учеб. для вузов по специальности "Приклад. информатика в экономике" А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко; Под ред. А. П. Пятибратова. - 3-е изд., перераб. и доп. - М.: Финансы и статистика, 2006. - 558, [1] с.
8. Автоматизированные информационные технологии в экономике [Текст] учеб. для вузов по агроэкон. специальностям М. И. Семенов, И. Т. Трубилин, В. И. Лойко, Т. П. Барановская ; под общ. ред. И. Т. Трубилина. - М.: Финансы и статистика, 1999. - 412, [1] с.

б) дополнительная литература:

1. Карабинцев, В. Г. Устранение угроз безопасности коммерческого объекта: Угрозы в организационной сфере. Собственная деловая разведка фирм - будущих партнеров. Собственная контрразведка и конкретизация деятельности службы безопасности. Взаимоотношения с контролирующими организациями. Физическая охрана объектов; предотвращение заказных убийств бизнесменов, захватов заложников. Полезные "хитрые" штучки на всякий случ Курс практ. рекомед. В. Г. Карабинцев. - Челябинск: Б. И., 1997. - 122 с.
2. Семенов, Ю. А. Алгоритмы телекоммуникационных сетей [Текст] Ч. 3 Процедуры, диагностика, безопасность учебное пособие : в 3 ч. Ю. А. Семенов. - М.: Интернет-Университет Информационных Технологий: БИНО, 2007
3. Лазарев, В. Е. Автоматизация бухгалтерского учета средствами системы "1 С: Предприятие" версий 7.5 и 7.7 Учеб. пособие Юж.-Урал. гос. ун-т, Каф. Двигатели внутр. сгорания; ЮУрГУ. - Челябинск: Издательство ЮУрГУ, 2000. - 64,[1] с. ил.

4. Гультяев, А. К. MATLAB 5.2: Имитационное моделирование в среде Windows: Визуализация. Программирование. Анализ данных. Практическое пособие. - СПб.: КОРОНА принт, 1999. - 287, [1] с. ил.
5. Безопасность жизнедеятельности. Безопасность технологических процессов и производств. Охрана труда [Текст] учеб. пособие для вузов П. П. Кукин и др. - Изд. 4-е, перераб. - М.: Высшая школа, 2007. - 334, [1] с. ил.
6. Безопасность жизнедеятельности. Безопасность технологических процессов и производств. Охрана труда [Текст] учеб. пособие для вузов П. П. Кукин, В. Л. Лапин, Е. А. Подгорных и др. - М.: Высшая школа, 1999. - 317, [1] с. ил.
7. Безопасность жизнедеятельности: Безопасность технологических процессов и производств: Охрана труда Учеб. пособие для вузов П. П. Кукин, В. Л. Лапин, Н. Л. Пономарев, Н. И. Сердюк. - 2-е изд., испр. и доп. - М.: Высшая школа, 2001. - 317, [1] с. ил.
8. Безопасность производственных процессов, машин и оборудования [Текст] А. В. Грачев и др.; Челяб. политехн. ин-т им. Ленинского комсомола, Каф. Охрана труда ; ЮУрГУ. - Челябинск: ЧПИ, 1983. - 39 с.
9. Белов, С. В. Безопасность жизнедеятельности и защита окружающей среды (техносферная безопасность) [Текст] учебник для вузов по дисциплине "Безопасность жизнедеятельности" для бакалавров С. В. Белов. - 4-е изд., перераб. и доп. - М.: Юрайт, 2013. - 681, [1] с. ил.
10. Крючек, Н. А. Безопасность и защита населения в чрезвычайных ситуациях Учеб.-метод. пособие для проведения занятий с населением Н. А. Крючек, В. Н. Латчук; Под ред. Г. Н. Кириллова; М-во Рос. Федерации по делам гражд. обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий. - М.: ЭНАС, 2001. - 145, [2] с.

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Конфидент. Защита информации.
2. Безопасность информационных технологий.

г) методические указания для студентов по освоению дисциплины:

1. Нормативные требования ФСТЭК России и ФСБ России в части формирования моделей угроз и моделей нарушителя.
2. Рагозин А. Н. Угрозы информационной безопасности автоматизированных систем. Методические указания к практическим занятиям. Челябинск 2016
3. ФГОС высшего образования по специальности 10.05.03 "Информационная безопасность автоматизированных систем"

из них: учебно-методическое обеспечение самостоятельной работы студента:

4. Нормативные требования ФСТЭК России и ФСБ России в части формирования моделей угроз и моделей нарушителя.

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в	Доступность (сеть Интернет /
---	----------------	-------------------------	------------------------	------------------------------

			электронной форме	локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Рагозин А. Н. Угрозы информационной безопасности автоматизированных систем. Методические указания к практическим занятиям. Челябинск 2016	Учебно-методические материалы кафедры	Локальная Сеть / Свободный
2	Основная литература	Основы информационной безопасности. [Электронный ресурс] : учеб. пособие / Е.Б. Белов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2006. — 544 с. — Режим доступа: http://e.lanbook.com/book/5121 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
3	Дополнительная литература	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. [Электронный ресурс] : учеб. пособие / А.А. Афанасьев [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 550 с. — Режим доступа: http://e.lanbook.com/book/5114 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. -Deductor Academic(бессрочно)
2. Math Works-MATLAB, Simulink 2013b(бессрочно)
3. -Maple 13(бессрочно)

Перечень используемых информационных справочных систем:

1. -База данных ВИНТИ РАН(бессрочно)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	913 (36)	Компьютерный класс