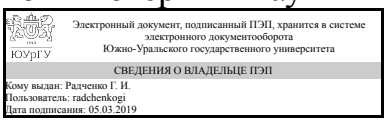
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



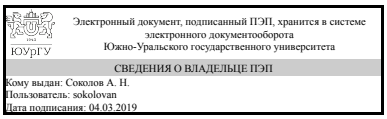
Г. И. Радченко

РАБОЧАЯ ПРОГРАММА
к ОП ВО от 26.06.2019 №084-2481

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

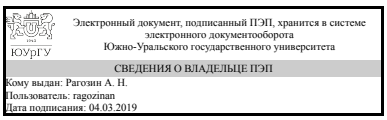
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

Разработчик программы,
к.техн.н., доцент



А. Н. Рагозин

Челябинск

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 критериев». 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
Аудиторные занятия:	48	48
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	24	24
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	60	60
Подгтовка к практическим занятиям	30	30
Подгтовка к зачёту	10	10
Подгтовка 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 поня-тия и определения. Понятие угрозы информационной безопасности.	6
2	2	Классификация угроз информационной безопасности. Основные категории угроз. Систем-ный 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 смстемного 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 зкспетгых систем оценки рисков с использованием нечёткой 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
Подглтовка к практическим занятиям	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., Зефиров 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.	30
Подглтовка к зачёту	1. Котенко И.В., Котухов М.М., Марков А.С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности	10

	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., Зефиров 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.	
Подглтовка рефератов	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.:	20

	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., Зефиров 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.	

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: Отвкт на олин 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	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	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	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

	рекомендации. 8 Нечеткие модели методы анализа информационных рисков.
Контрольные вопросы и задания для проведения текущего контроля	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	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. Корченко, А. Г. Построение систем защиты информации на нечетких множествах: Теория и практические решения А. Г. Корченко. - Киев: МК-Пресс, 2006. - 316 с. ил.

2. Информационная безопасность и защита информации Текст учеб. пособие для студентов вузов по направлению 230200 "Информ. системы" специальности 230201 "Информ. системы и технологии" Ю. Ю. Громов и др. - Старый Оскол: Тонкие наукоемкие технологии, 2010. - 383 с. ил., табл.

3. Баранова, Е. К. Информационная безопасность и защита информации Текст учеб. пособие по направлению "Приклад. информатика" Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - М.: РИОР : ИНФРА-М, 2016. - 320, [1] с. ил.

4. Краковский, Ю. М. Информационная безопасность и защита информации Текст учеб. пособие по специальности "Информ. системы и технологии" дневной и заоч. форм обучения Ю. М. Краковский. - М.; Ростов н/Д: Март, 2008. - 287 с. 22 см.

5. Мельников, В. П. Информационная безопасность и защита информации Текст учеб. пособие В. П. Мельников и др.; под ред. С. А. Клейменова. - 4-е изд., стер. - М.: Академия, 2009. - 330, [1] с.

6. Петренко, С. А. Управление информационными рисками : Экономически оправданная безопасность Текст С. А. Петренко, С. В. Симонов. - М.: Академия АйТи: ДМК Пресс, 2004. - 383 с. ил.

7. Обеспечение информационной безопасности бизнеса А. П. Курило, С. Г. Антимонов, В. В. Андрианов и др. - М.: БДЦ-Пресс, 2005. - 511 с.

8. Основы управления информационной безопасностью Текст учеб. пособие для вузов по направлениям (специальностям) 090000 "Информ. безопасность" А. П. Курило и др. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2016. - 243 с. ил.

б) дополнительная литература:

1. Управление рисками Исполн. ред. Д. Пикфорд; Пер. с англ. О. Н. Матвеевой; Под ред. О. Ю. Анисимова. - М.: Вершина, 2004. - 349, [2] с. ил.

2. Рутковская, Д. Нейронные сети, генетические алгоритмы и нечеткие системы Текст Д. Рутковская, М. Пилиньский, Л. Рутковский ; пер. с пол. И. Д. Рудинского. - 2-е изд., стер. - М.: Горячая линия - Телеком, 2013. - 383 с. ил.

3. Хайкин, С. Нейронные сети Полный курс С. Хайкин; Пер. с англ. Н. Н. Куссуль, А. Ю. Шелестова. - 2-е изд. - М. и др.: Вильямс, 2006. - 1103 с.

4. Яхъяева, Г. Э. Нечеткие множества и нейронные сети Текст учеб. пособие Г. Э. Яхъяева. - 2-е изд., испр. - М.: Интернет-Университет Информационных Технологий : БИНО, 2008

5. Яхъяева, Г. Э. Нечеткие множества и нейронные сети Учеб. пособие Г. Э. Яхъяева. - М.: Интернет-Университет Информационных Технологий: БИНО, 2006

6. Ярочкин, В. И. Аудит безопасности фирмы : теория и практика Текст учебное пособие для вузов В. И. Ярочкин, Я. В. Бузанова. - М.; Королев: Академический проект : Парадигма, 2005. - 350, [1] с.

7. Ярочкин, В. И. Информационная безопасность Текст учеб. для вузов по гуманитар. и социал.-экон. специальностям В. И. Ярочкин. - 4-е изд. - М.: Академический проект, 2006. - 542, [1] с. ил.

8. Нейронные сети. Statistica Neural Networks Пер. с англ. StatSoft Russia. - М.: Горячая линия-Телеком: Грааль, 2000

9. Головко, В. А. Нейронные сети: Обучение, организация и применение Учеб. пособие по направлению подготовки бакалавров и магистров "Приклад. математика и физика" В. А. Головко; Под общ. ред. А. И. Галушкина. - М.: ИПРЖР, 2001. - 256 с. ил.

10. Круглов, В. В. Искусственные нейронные сети: Теория и практика В. В. Круглов, В. В. Борисов. - 2-е изд., стер. - М.: Горячая линия-Телеком, 2002

11. Медведев, В. С. Нейронные сети: Matlab 6 В. С. Медведев, В. Г. Потемкин; Под общ. ред. В. Г. Потемкина. - М.: ДИАЛОГ-МИФИ, 2002. - 489 с. ил.

12. Осовский, С. Нейронные сети для обработки информации С. Осовский; Пер. с пол. И. Д. Рудинского. - М.: Финансы и статистика, 2002. - 343 с. ил.

13. Рутковская, Д. Нейронные сети, генетические алгоритмы и нечеткие системы Д. Рутковская, М. Пилиньский, Л. Рутковский; Пер. с пол. И. Д. Рудинского. - М.: Горячая линия -Телеком, 2006

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 электронной форме	Доступность (сеть Интернет / 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	ЛокальнаяСеть / Свободный
2	Основная литература	Основы информационной безопасности. [Электронный ресурс] : учеб. пособие / Е.Б. Белов [и др.]. — Электрон. дан. — М. :	Электронно-библиотечная система	Интернет / Авторизованный

		Горячая линия-Телеком, 2006. — 544 с. — Режим доступа: http://e.lanbook.com/book/5121 — Загл. с экрана.	издательства Лань	
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 ВИНИТИ 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 (3б)	Компьютерный класс