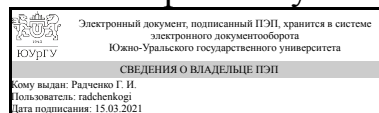


# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:  
Директор института  
Высшая школа электроники и  
компьютерных наук



Г. И. Радченко

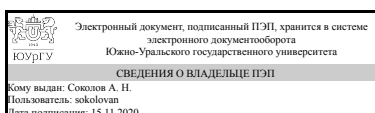
## РАБОЧАЯ ПРОГРАММА

дисциплины В.1.08 Основы аттестации объектов информатизации критически важных объектов  
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

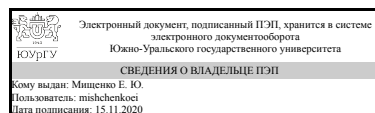
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

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



А. Н. Соколов

Разработчик программы,  
старший преподаватель



Е. Ю. Мищенко

## 1. Цели и задачи дисциплины

Цель - освоение технологий аттестации объектов информатизации критически важных объектов. Задачи: освоение базовых понятий в области аттестации объектов информатизации критически важных объектов; изучение нормативной правовой базы аттестации объектов информатизации критически важных объектов; знакомство с организационной структурой аттестации объектов информатизации; поэтапное освоение методики аттестации объектов информатизации; изучение системы документационного обеспечения аттестации объектов информатизации; освоение специфики аттестации объектов информатизации критически важных объектов.

## Краткое содержание дисциплины

В рамках дисциплины изучаются базовые понятия в области аттестации объектов информатизации критически важных объектов; нормативная правовая базы по аттестации объектов информатизации, в том числе - критически важных объектов; организационная структура аттестации объектов информатизации; этапы аттестации объектов информатизации; система документационного обеспечения аттестации объектов информатизации; специфики аттестации объектов информатизации критически важных объектов.

## 2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Знать: Требования к этапам ввода и вывода из эксплуатации системы защиты информации
	Уметь: Разрабатывать заключение по результатам аттестационных испытаний
	Владеть:
ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	Знать: Требования нормативных документов к составу, содержанию и оформлению технической документации объекта информатизации
	Уметь: Разрабатывать техническую документацию объекта информатизации
	Владеть: Навыками организации и планирования процесса аттестации
ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	Знать: Регламент проведения аттестационных испытаний
	Уметь: Разрабатывать программу и методики аттестационных испытаний
	Владеть: Методами проведения аттестационных испытаний
ПСК-3.5 способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов	Знать: Требования защиты информации к аттестованным объектам
	Уметь:
	Владеть: Навыками мониторинга изменения состояния аттестованного объекта

### 3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.21 Программно-аппаратные средства обеспечения информационной безопасности, Б.1.23 Криптографические методы защиты информации	Производственная практика, преддипломная практика (10 семестр)

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

Дисциплина	Требования
Б.1.23 Криптографические методы защиты информации	механизмы криптографических средств защиты информации
Б.1.21 Программно-аппаратные средства обеспечения информационной безопасности	механизмы защиты программно-аппаратных средств защиты информации

### 4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		9	
Общая трудоёмкость дисциплины	144	144	
<i>Аудиторные занятия:</i>	64	64	
Лекции (Л)	32	32	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	80	80	
Разработка базы данных "Система документации по аттестации ОИ КВО"	80	80	
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен	

### 5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Аттестация объектов информатизации критически важных объектов: базовые понятия, общая характеристика	6	6	0	0
2	Нормативная правовая база по аттестации объектов информатизации, в том числе - критически важных объектов	6	6	0	0
3	Организационная структура аттестации объектов информатизации в России	4	4	0	0
4	Этапы аттестации объектов информатизации критически	28	6	22	0

	важных объектов и их реализация				
5	Документационное сопровождение аттестации объектов информатизации критически важных объектов	20	10	10	0

## 5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Базовые понятия аттестации объектов информатизации КВО	4
2	1	Общая характеристика процесса аттестации ОИ КВО	2
3	2	Нормативная правовая база по аттестации объектов информатизации	4
4	2	Нормативная правовая база по аттестации объектов информатизации критически важных объектов	2
5	3	Организационная структура аттестации ОИ: общая характеристика	2
6	3	Организационная структура системы аттестации ОИ в РФ: характеристика отдельных подсистем	2
7	4	Этапы аттестации ОИ КВО: общая характеристика	2
8	4	Подача заявки на рассмотрение и проведение аттестации. Анализ исходных данных по аттестуемому объекту информатизации. Проведение предварительного специального обследования аттестуемого объекта информатизации. Разработка программы и методики аттестационных испытаний. Заключение договоров на аттестацию. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте	2
9	4	Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации. Проведение аттестационных испытаний ОИ. Оформление, регистрация и выдача «Аттестата соответствия». Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных ОИ. Рассмотрение апелляций.	2
10	5	Система документационного сопровождения аттестации ОИ КВО: общая характеристика	4
11	5	Заключение аттестационной проверки, Протокол аттестационных испытаний, «Аттестат соответствия» на объект информатизации, отвечающий требованиям по безопасности информации: Структура, содержание.	4
12	5	Специфика процедуры аттестации ОИ КВО	2

## 5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	4	Подача заявки на рассмотрение и проведение аттестации. Анализ исходных данных по аттестуемому объекту информатизации.	4
2	4	Проведение предварительного специального обследования аттестуемого объекта информатизации. Разработка программы и методики аттестационных испытаний	4
3	4	Заключение договоров на аттестацию. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте.	2
4	4	Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации.	2

5	4	Проведение аттестационных испытаний объекта информатизации.	4
6	4	Оформление, регистрация и выдача «Аттестата соответствия»	4
7	4	Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации. Рассмотрение апелляций.	2
8	5	Заключение аттестационной проверки: структура, содержание	4
9	5	Протокол аттестационного испытания	4
10	5	Аттестат соответствия ОИ КВО требованиям безопасности	2

### 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
Разработка базы данных "Система документации по аттестации ОИ КВО"	Положение по аттестации объектов информатизации по требованиям безопасности информации. (Утверждено Председателем Гостехкомиссии России 25.11.1994). – М.: Гостехкомиссия РФ, 1994.	80

## 6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
анализ НМД	Лекции	анализ преимуществ и недостатков практического применения НМД	10

## Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
Использование проектных технологий комплексного решения практических задач	Проектирование БД "СД по аттестации ОИ КВО"

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	Контролируемая компетенция ЗУНЫ	Вид	№№
--------------	---------------------------------	-----	----

разделов дисциплины		контроля (включая текущий)	заданий
Все разделы	ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	экзамен	1-50 и 1-30 тест
Все разделы	ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	экзамен	1-50 и 1-30 тест

## 7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
экзамен	студенты в аудитории письменно отвечают на вопросы экзаменационного билета, который включает теоретический, практический вопросы и один вопрос из теста по пройденным разделам, преподаватель проверяет, беседует и оценивает	Отлично: даны полные, развёрнутые ответы на теоретический, практический вопросы и один вопрос из теста по пройденным разделам Хорошо: даны либо неполные ответы на теоретический, практический вопросы и один вопрос из теста, либо при полных ответах на два вопроса дан неправильный ответ на вопрос теста Удовлетворительно: даны либо неполные ответы на теоретический или практический вопрос и неправильный ответ на вопрос теста, либо при одном полном ответе даны два неправильных ответа на остальные вопросы Неудовлетворительно: даны либо неполные ответы на теоретический или практический вопрос и неправильные ответы на два остальных вопроса, либо даны неправильные ответы на все три вопроса

## 7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
экзамен	см. файлы Экзамен аттестация ОИ.docx; 3 Тесты аттестация.docx

## 8. Учебно-методическое и информационное обеспечение дисциплины

### Печатная учебно-методическая документация

#### а) основная литература:

1. Организационно-правовое обеспечение информационной безопасности Текст учеб. пособие для вузов по специальностям 090102 "Компьютер. безопасность" и др. А. А. Стрельцов и др.; под ред. А. А. Стрельцова. - М.: Академия, 2008. - 248, [1] с. ил., табл.

2. 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.

3. Родичев, Ю. А. Информационная безопасность : нормативно-правовые аспекты Текст учеб. пособие по специальностям 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информ. безопасности автоматиз. систем" Ю. А. Родичев. - СПб. и др.: Питер, 2008. - 271, [1] с.

*б) дополнительная литература:*

1. ГОСТ Р 51275-2006 : Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения : утв. и введ. в действие от 27.12.06 : взамен ГОСТ Р 51275-99 Текст Федер. агентство по техн. регулированию и метрологии. - М.: Стандартинформ, 2007. - 7 с.

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

1. Защита информации. Инсайд ,информ.-метод. журн. ,Изд. дом "Афина"

2. Защита информации. Конфидент / Ассоц. защиты информ. "Конфидент" : информ.-метод. журн

3. БДИ: Безопасность. Достоверность. Информация рос. журн. о безопасности бизнеса и личности ООО "Журн. "БДИ" журнал"

4. Безопасность информационных технологий ,М-во образования и науки Рос. Федера-ции, Моск. инж.-физ. ин-т (гос. ун-т), ВНИИПВТИ

5. Вестник УрФО : Безопасность в информационной сфере ,Юж.-Урал. гос. ун-т; ЮУрГУ

*г) методические указания для студентов по освоению дисциплины:*

1. Аттестация объектов информатизации конспект

*из них: учебно-методическое обеспечение самостоятельной работы студента:*

**Электронная учебно-методическая документация**

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: <a href="http://e.lanbook.com/book/5163">http://e.lanbook.com/book/5163</a> — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

2	Дополнительная литература	ГОСТ Р 51275-2006 : Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения	Консультант плюс	Интернет / Свободный
---	---------------------------	----------------------------------------------------------------------------------------------------------------------	------------------	----------------------

## 9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. -Консультант Плюс(31.07.2017)
2. -Стандартинформ(бессрочно)

## 10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт. ), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Консультант+.
Практические занятия и семинары	910 (3б)	Комплект компьютерного оборудования, Стенд по методам и средствам защиты телефонных аппаратов и телефонных линий, Стенд по биометрическим способам индикации, Стенд по противопожарной защите, Стенд по системам аналогового видеонаблюдения, Стенд по системам цифрового видеонаблюдения, Стенд по техническим средствам охраны на базе приборов «Сигнал 20» и «Сигнал 20 П», Стенд по техническим средствам охраны на базе контроллера «С200-КФЛ», Переносной комплекс для измерений «Навигатор ПЗГ», Комплекс контроля эффективности защиты речевой информации «Спрут-мини-А», Лабораторный стенд для исследования линий связи, Селективный микровольтметр, Осциллограф С1-65, Генератор импульсов Г5-54, Аппаратный шифратор, Поисковый комплекс «Пиранья», Нелинейный локатор «Родник-2К», Детектор поля, Устройство комбинированной защиты, настенные информационные стенды (3 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozilla Firefox, Орион, VidioNET.