

МИНОБРНАУКИ РОССИИ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
**«Российский государственный гуманитарный университет»  
(РГГУ)**

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ  
Факультет информационных систем и безопасности  
Кафедра информационной безопасности

## **ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

По направлению подготовки 10.03.01 «Информационная безопасность»  
профиль «Организация и технология защиты информации»

Уровень квалификации выпускника (*бакалавр*)  
Форма обучения (*очная*)

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2017

Организационное обеспечение аттестации объектов информатизации  
Рабочая программа дисциплины

Составитель:

д.т.н, профессор В.В. Арутюнов

Ответственный редактор

к.и.н., доцент, заведующая кафедрой

информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО

Протокол заседания кафедры информационной безопасности

№ 5 от 24.01.2017

## ОГЛАВЛЕНИЕ

### **1. Пояснительная записка**

1.1 Цель и задачи дисциплины (*модуля*)

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине (*модулю*)

1.3. Место дисциплины в структуре образовательной программы

### **2. Структура дисциплины (*модуля*)**

### **3. Содержание дисциплины (*модуля*)**

### **4. Образовательные технологии**

### **5. Оценка планируемых результатов обучения**

5.1. Система оценивания

5.2. Критерии выставления оценок

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (*модулю*)

### **6. Учебно-методическое и информационное обеспечение дисциплины**

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети Интернет

### **7. Материально-техническое обеспечение дисциплины (*модуля*)**

### **8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

### **9. Методические материалы**

9.1. Планы практических (семинарских, лабораторных) занятий

### **10. Методические рекомендации по организации самостоятельной работы**

## **Приложения**

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины (модуля)

Целью курса является формирование навыков организации проведения комплекса организационно-технических мероприятий (аттестационных испытаний), в результате которых устанавливается соответствие защищаемого объекта требованиям стандартов и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Задачи: анализ функций органов аттестации, испытательных центров, заявителей и их взаимодействие при проведении аттестации объектов информатизации; изучение порядка проведения аттестации (разработка заявки на проведение аттестации, программы и методики аттестационных испытаний, их проведение), оформления и регистрации аттестата соответствия.

### 1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине (модулю):

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	знать: основные нормативно-правовые документы в профессиональной деятельности; уметь: пользоваться нормативно-правовыми документами в области защиты информации; владеть: навыками работы с нормативно-правовыми документами в сфере защиты информации.
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	знать: организацию проведения и сопровождение аттестации объекта на соответствие требованиям государственных нормативных документов; уметь: оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности владеть: профессиональной терминологией
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	знать: виды и формы информации, подверженной угрозам уметь: проводить предварительный технико-экономический анализ и обоснования проектных решений по обеспечению информационной безопасности; владеть: навыками использования технических средств в профессиональной деятельности

ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы по техническому и экспортному контролю	знать: организацию аттестации объектов по требованиям безопасности информации; уметь: формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административной и технической реализуемости и экономической целесообразности; владеть: способами организации и проведения (сопровождения) аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов;
-------	--	---

### 1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Организационное обеспечение аттестации объектов информатизации» относится к вариативной части блока дисциплин учебного плана.

Для освоения дисциплины (модуля) необходимы компетенции, сформированные в ходе изучения следующих дисциплин и прохождения практики: Методы принятия организационно-технических решений, Защита информации от несанкционированного доступа, Экономика защиты информации.

В результате освоения дисциплины (модуля) формируются компетенции, необходимые для изучения следующих дисциплин и прохождения практики: Аудит информационной безопасности, Системы информационно-аналитического мониторинга.

## 2. Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся - 44 ч.

№ п/ п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
			контактная					Самостоятель- ная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Назначение и общая характеристика аттестации и сертификации в области защиты информации	7	4		2			8	опрос
2	Основные требования к защищённости базовых объектов информатизации	7	4		2			8	опрос
3	Организационная	7	4		2			14	опрос

	структура системы аттестации объектов информатизации по требованиям безопасности информации								
4	Порядок проведения аттестации объектов информатизации	7	4		6			14	опрос, контрольная работа
5	зачет								Зачет по билетам
	Итого		16		12			44	

### 3. Содержание дисциплины (модуля)

#### Тема 1. Назначение и общая характеристика аттестации и сертификации в области защиты информации

Предмет и содержание дисциплины, методы изучения, основная литература, контроль освоения дисциплины.

Основные цели механизмов лицензирования и сертификации в России. Базовый нормативный документ в области сертификации и аттестации в России.

Цели и принципы сертификации. Понятие декларации о соответствии и обязательной сертификации. Содержание декларации о соответствии.

Сущность и состав сертификата соответствия. Основные схемы декларирования соответствия продукции. Основные принципы проведения сертификационных испытаний средств защиты информации. Сертификация продукции на международном уровне.

#### Тема 2. Основные требования к защищённости базовых объектов информатизации

Основная цель аттестации объектов информатизации. Базовые нормативные правовые акты в сфере сертификации и аттестации. Основные схемы аттестации объектов информатизации.

Аттестация автоматизированных систем и средств вычислительной техники (СВТ) в России в соответствии с руководящими документами (РД) ФСТЭК России. Перечень требований к защищённости автоматизированных систем в зависимости от класса защищённости. Перечень требований к защищённости СВТ в зависимости от класса защищённости.

Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недеklarированных возможностей.

Классификация межсетевых экранов по уровню защищённости от НСД.

#### Тема 3. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации

Основные элементы системы аттестации объектов информатизации по требованиям безопасности информации. Структура органов по аттестации объектов информатизации, которые аккредитуются ФСТЭК России. Основные функции

федерального органа по сертификации и аттестации. Базовые функции органов по аттестации объектов информатизации.

Основные работы испытательных центров (лабораторий) по сертификации продукции. Базовые виды работ заявителей аттестуемых объектов информатизации.

#### **Тема 4. Порядок проведения аттестации объектов информатизации**

Основные этапы проведения аттестации объектов информатизации. Содержание, порядок государственного контроля и надзора по аттестации объектов информатизации.

Содержание заявки заявителя для получения «Аттестата соответствия». Порядок проведения аттестационных испытаний. Исходные данные и документация, представляемая заявителем органу по аттестации.

Основные работы при проведении специального обследования аттестуемого объекта. Базовые работы, проводимые при аттестации объектов информатизации для каждого технического средства обработки информации (ТСОИ). Основные работы при аттестации выделенного помещения.

Структура заключения аттестационной проверки объекта информатизации. Содержание протокола аттестационных испытаний. Структура «Аттестата соответствия» объекта информатизации (выделенного помещения) требованиям по безопасности информации. Сущность контроля состояния защиты информации с целью своевременного выявления и предотвращения утечки информации по техническим каналам на предприятии. Категорирование объектов и определение режимных зон внутри них.

#### **4. Образовательные технологии**

При реализации рабочей программы дисциплины используются следующие информационные и образовательные технологии:

<b>№ п/п</b>	<b>Наименование раздела</b>	<b>Виды учебной работы</b>	<b>Информационные и образовательные технологии</b>
1.	Назначение и общая характеристика аттестации и сертификации в области защиты информации	Лекция 1  Семинар 1	Вводная лекция с использованием видеоматериалов  опрос
2.	Основные требования к защищённости базовых объектов информатизации	Лекция 2  Семинар 2	Лекция с использованием видеопроектора  опрос
3.	Организационная структура системы аттестации объектов информатизации по	Лекция 3	Лекция с использованием видеопроектора

	требованиям безопасности информации	Семинар 3	опрос
4.	Порядок проведения аттестации объектов информатизации	Лекция 4 Семинар 4 Контрольная работа	Лекция с использованием видеопроектора Опрос Подготовка к контрольной с использованием материалов лекций и литературы

## 5. Оценка планируемых результатов обучения

### 5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: - <i>опрос</i> - <i>контрольная работа (темы 3-4)</i>	<i>10 баллов</i> <i>20 баллов</i>	<i>40 баллов</i> <i>20 баллов</i>
Промежуточная аттестация (традиционная форма)		<i>40 баллов</i>
<b>Итого за семестр зачёт</b>		<i>100 баллов</i>

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представлен в виде таблицы:

№ п/п	Контролируемые разделы дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1.	1	ОПК-5, ПК-15	опрос
2.	2	ПК-10, ПК-5	опрос
3.	3	ОПК-5, ПК-15	опрос
4.	4	ПК-5, ПК-10	опрос контрольная работа

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

Оценка «зачёт» выставляется обучающемуся, набравшему не менее 50 баллов в результате суммирования баллов, полученных при текущем контроле и промежуточной аттестации. Полученный совокупный результат (максимум 100 баллов) конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и



накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

10

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

## 5.2.Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	зачтено	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	зачтено	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
67-50/ D, E	зачтено	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F, FX	не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

***Текущий контроль (вариант опросного задания)***

***Примерная тематика вопросов для опроса:***

<b><i>Вопросы</i></b>	<b><i>Реализуемая компетенция</i></b>
1. Базовые органы - генераторы правовых документов в сфере ИБ в России на федеральном уровне	<b><i>ОПК-5</i></b>
2. Объекты информатизации, аттестуемые по требованиям безопасности информации.	<b><i>ПК-5</i></b>

3. Основные виды работ, проводимые в соответствии со схемой аттестации.	<b>ПК-15</b>
4. Базовые категории аттестуемых объектов информатизации	<b>ПК-10</b>

12

***Примерная тематика контрольной работы - проверка  
сформированности компетенций ОПК-5, ПК-5, ПК-10, ПК-15***

1. Содержание декларации о соответствии.
2. Особенности различных схем декларирования соответствия продукции.
3. Содержание сертификата соответствия.
4. Сведения, содержащиеся в сертификате на продукцию.
5. Базовые уровни сертификации для систем конфиденциального электронного документооборота.
6. Основные виды документов, используемые при проведении сертификационных испытаний. .
7. Базовые разделы методики сертификационных испытаний.
8. Содержание протокола сертификационных испытаний.
9. Основные группы классификация автоматизированных систем в соответствии с требованиями по защите информации.
10. Базовые группы показателей защищённости СВТ.
11. Основные группы требований к защищённости АС в зависимости от класса их защищённости.
12. Классификация МЭ по уровню контроля отсутствия незадекларированных возможностей.
13. Функции органов по аттестации объектов информатизации.
14. Состав программы аттестационных испытаний.
15. Базовые действия при аттестации выделенного помещения.
16. Основные разделы протокола аттестационных испытаний.

***Промежуточная аттестация (примерные контрольные вопросы по курсу) -  
проверка сформированности компетенций ОПК-5, ПК-5, ПК-10, ПК-15***

1. Основные цели сертификации в России в области защиты информации.
2. Характеристика базовых органов - генераторов правовых документов в сфере ИБ в России на федеральном уровне.

3. Основные принципы, обеспечивающие эффективность сертификации.
4. Содержание декларации о соответствии.
5. Особенности различных схем декларирования соответствия продукции.
6. Основные принципы проведения сертификационных испытаний средств защиты информации.
7. Основные разделы пользовательской документации для импортного ПО.
8. Базовые объекты информатизации, аттестуемые в соответствии с требованиями безопасности информации.
9. Основные виды работ, проводимые в соответствии со схемой аттестации.
10. Перечень необходимых работ для выбора схемы аттестации.
11. Классификация автоматизированных систем в соответствии с требованиями по защите информации.
12. Классификация СВТ в соответствии с требованиями по защите информации.
13. Основные требования по защите, предъявляемые к межсетевым экранам.
14. Классификация программного обеспечения по уровню контроля отсутствия недеklarированных возможностей.
15. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.
16. Основные работы заявителей для проведения аттестации объектов информатизации.
17. Базовые этапы проведения аттестации.
18. Содержание программы аттестационных испытаний.
19. Основные категории аттестуемых объектов информатизации.
20. Базовые зоны безопасности аттестуемых объектов информатизации.

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **6.1. Список источников и литературы**

#### **а) основная литература**

1. Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: <https://www.intuit.ru/studies/courses/3648/890/info>
2. Положение по аттестации объектов информатизации по требованиям безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL:

<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=>

б) дополнительная литература

1. Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: [https://elibrary.ru/download/elibrary\\_27692421\\_57961861.pdf](https://elibrary.ru/download/elibrary_27692421_57961861.pdf)

2. Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: <https://moluch.ru/archive/52/>

6.2. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимый для освоения дисциплины (модуля)

1. Информационный портал в области защиты информации - Режим доступа: <http://www.securitylab.ru>

2. Портал ФСТЭК России - Режим доступа: <http://fstec.ru>

3. Национальный открытый университет ИНТУИТ - Режим доступа: <http://www.intuit.ru>

4. Государственная публичная научно-техническая библиотека России - Режим доступа: <http://www.gpntb.ru>

6.3. Перечень БД и ИСС

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

## 7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен Microsoft Office 2010, включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

### Перечень ПО

№ п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

### 8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
  - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
  - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
  - письменные задания оформляются увеличенным шрифтом;
  - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих:
  - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
  - письменные задания выполняются на компьютере в письменной форме;
  - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
  - в печатной форме увеличенным шрифтом;
  - в форме электронного документа;
  - в форме аудиофайла.
- для глухих и слабослышащих:
  - в печатной форме;
  - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - в печатной форме;
  - в форме электронного документа;
  - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;

- принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - передвижными, регулируемые эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

## **9. Методические материалы**

### **9.1. Планы практических занятий - проверка сформированности компетенций ОПК-5, ПК-5, ПК-10, ПК-15**

#### **Планы практических занятий**

**Практическое занятие 1. (Тема 1). Цели осуществления сертификации в России - (2 часа) - проверка сформированности компетенций ОПК-5, ПК-5**

#### **Вопросы для изучения и обсуждения:**

1. Базовые цели реализации сертификации в России.
2. Основные уровни сертификации для систем конфиденциального электронного документооборота.
3. Базовые органы - генераторы правовых документов в сфере ИБ в России на федеральном уровне.
4. Основные принципы, соблюдение которых необходимо при проведении сертификационных испытаний средств защиты информации.

#### **Контрольные вопросы:**

1. Понятие декларации о соответствии.
2. Основные документы, необходимые для регистрации системы добровольной сертификации.
3. Структура сертификата соответствия.
4. Содержание декларации о соответствии.

Список литературы:

Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: <https://www.intuit.ru/studies/courses/3648/890/info>

Положение по аттестации объектов информатизации по требованиям безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL:



<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=>

Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: [https://elibrary.ru/download/elibrary\\_27692421\\_57961861.pdf](https://elibrary.ru/download/elibrary_27692421_57961861.pdf)

Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: <https://moluch.ru/archive/52/>

Информационный портал в области защиты информации - Режим доступа: <http://www.securitylab.ru>

Портал ФСТЭК России - Режим доступа: <http://fstec.ru>

Национальный открытый университет ИНТУИТ - Режим доступа: <http://www.intuit.ru>

Государственная публичная научно-техническая библиотека России - Режим доступа: <http://www.gpntb.ru>

**Практическое занятие 2. (Тема 2).** Аттестация автоматизированных систем, средств вычислительной техники и межсетевых экранов в России - **(2 часа) - проверка сформированности компетенций - ПК-10, ПК15**

**Вопросы для изучения и обсуждения:**

1. Основные схемы проведения аттестации объектов информатизации.
2. Базовые классы защищённости автоматизированных систем.
3. Основные группы защищённости СВТ.
4. Классификация программного обеспечения по уровню контроля отсутствия недекларированных возможностей.
5. Перечень требований защищённости СВТ.
6. Классификация межсетевых экранов по уровню защищённости от НСД.

**Контрольные вопросы:**

1. Понятие аттестации объектов информатизации.
2. Перечислите основные объекты информатизации, подлежащие аттестации.
3. В каких случаях аттестация носит обязательный или добровольный характер?
4. Перечислите нормативные правовые акты, определяющие основные принципы и

организационную структуру системы аттестации и порядок проведения аттестации.

5. Основные требования по защите межсетевых экранов.

19

6. Перечислите основные подсистемы автоматизированных систем, для которых устанавливаются требования по их защищённости.

#### **Список литературы:**

Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: <https://www.intuit.ru/studies/courses/3648/890/info>

Положение по аттестации объектов информатизации по требованиям безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL:

<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=>

Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: [https://elibrary.ru/download/elibrary\\_27692421\\_57961861.pdf](https://elibrary.ru/download/elibrary_27692421_57961861.pdf)

Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: <https://moluch.ru/archive/52/>

Портал ФСТЭК России - Режим доступа: <http://fstec.ru>

Национальный открытый университет ИНТУИТ - Режим доступа: <http://www.intuit.ru>

**Практическое занятие 3. (Тема 3). Основные элементы системы аттестации объектов информатизации по требованиям безопасности информации - (2 часа) - проверка сформированности компетенций - ПК-5, ПК-15**

#### **Вопросы для изучения и обсуждения:**

1. Структурный состав системы аттестации объектов информатизации по требованиям безопасности информации.
2. Основные элементы органов по аттестации объектов информатизации.
3. Базовые функции федерального органа по сертификации и аттестации.
4. Основные функции органов по аттестации объектов информатизации.

#### **Контрольные вопросы:**

1. Перечислите элементы системы аттестации объектов информатизации по требованиям безопасности информации.
2. Основные работы заявителей для проведения аттестации объектов информатизации.
3. Какую работу проводят испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации?
4. Основные разделы заявки заявителя на проведение аттестации.

Список литературы:

Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: <https://www.intuit.ru/studies/courses/3648/890/info>

Положение по аттестации объектов информатизации по требованиям безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=>

Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: [https://elibrary.ru/download/elibrary\\_27692421\\_57961861.pdf](https://elibrary.ru/download/elibrary_27692421_57961861.pdf)

Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: <https://moluch.ru/archive/52/>

Портал ФСТЭК России - Режим доступа: <http://fstec.ru>

Национальный открытый университет ИНТУИТ - Режим доступа: <http://www.intuit.ru>

**Практическое занятие 4. (Тема 4). Основные этапы проведения аттестации объектов информатизации - (2 часа) - проверка сформированности компетенций - ПК-10, ПК-15**

**Вопросы для изучения и обсуждения:**

1. Сведения, представляемые заявителем для проведения аттестационных испытаний.
2. Основные работы, проводимые при проведении специального обследования аттестуемого объекта.
3. Базовые работы, проводимые при аттестации выделенного помещения.
4. Содержание программы аттестационных испытаний.
5. Основные категории аттестуемых объектов информатизации.

### Контрольные вопросы:

1. Перечислите этапы проведения аттестации объектов информатизации.
2. Что реализуется на начальном этапе проведения аттестации объектов информатизации?
3. Что включает этап проведения аттестационных испытаний объекта информатизации?
4. Основные разделы заявки заявителя на получение «Аттестата соответствия».
5. Содержание протокола аттестационных испытаний.

Список литературы:

Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: <https://www.intuit.ru/studies/courses/3648/890/info>

Положение по аттестации объектов информатизации по требованиям безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=>

Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: [https://elibrary.ru/download/elibrary\\_27692421\\_57961861.pdf](https://elibrary.ru/download/elibrary_27692421_57961861.pdf)

Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: <https://moluch.ru/archive/52/>

Портал ФСТЭК России - Режим доступа: <http://fstec.ru>

Национальный открытый университет ИНТУИТ - Режим доступа: <http://www.intuit.ru>

### 10. Методические указания для обучающихся по освоению дисциплины (модуля)

Трудоемкость освоения дисциплины «Организационное обеспечение аттестации объектов информатизации» составляет 72 часа, из них 44 часа отведены на самостоятельную работу студента (СР).

Вид работы	Содержание (перечень вопросов)	Трудоем- кость самостоя- тельной работы (в часах)	Рекомендации
------------	-----------------------------------	--	--------------

<p>Подготовка к практическому занятию Тема 1. «Назначение и общая характеристика аттестации и сертификации в области защиты информации»</p>	<p>Базовые цели реализации сертификации в России.</p> <p>Основные уровни сертификации для систем конфиденциального электронного документооборота.</p> <p>Базовые органы - генераторы правовых документов в сфере ИБ в России на федеральном уровне.</p> <p>Основные принципы, соблюдение которых необходимо при проведении сертификационных испытаний средств защиты информации.</p>	<p>8</p>	<p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: <a href="https://www.intuit.ru/studies/courses/3648/890/info">https://www.intuit.ru/studies/courses/3648/890/info</a></p> <p>Положение по аттестации объектов информатизации по требованиям безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL: <a href="https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=">https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=</a></p> <p>Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: <a href="https://elibrary.ru/download/elibrary_27692421_57961861.pdf">https://elibrary.ru/download/elibrary_27692421_57961861.pdf</a></p> <p>Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности</p>
---	--	----------	---

			<p>информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: <a href="https://moluch.ru/archive/52/">https://moluch.ru/archive/52/</a></p> <p>Информационный портал в области защиты информации - Режим доступа: <a href="http://www.securitylab.ru">http://www.securitylab.ru</a></p> <p>Портал ФСТЭК России - Режим доступа: <a href="http://fstec.ru">http://fstec.ru</a></p> <p>Национальный открытый университет ИНТУИТ - Режим доступа: <a href="http://www.intuit.ru">http://www.intuit.ru</a></p> <p>Государственная публичная научно-техническая библиотека России - Режим доступа: <a href="http://www.gpntb.ru">http://www.gpntb.ru</a></p>
Подготовка к практическому занятию Тема 2. «Аттестация автоматизированных систем, средств вычислительной техники и межсетевых экранов в России»			<p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: <a href="https://www.intuit.ru/studies/courses/3648/890/info">https://www.intuit.ru/studies/courses/3648/890/info</a></p> <p>Положение по аттестации объектов информатизации по требованиям безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL: <a href="https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-">https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-</a></p>

			<p>polozhenie-ot-25-noyabrya-1994-g?highlight=</p> <p>Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: <a href="https://elibrary.ru/download/elibrary_27692421_57961861.pdf">https://elibrary.ru/download/elibrary_27692421_57961861.pdf</a></p> <p>Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: <a href="https://moluch.ru/archive/52/">https://moluch.ru/archive/52/</a></p> <p>Портал ФСТЭК России - Режим доступа: <a href="http://fstec.ru">http://fstec.ru</a></p> <p>Национальный открытый университет ИНТУИТ - Режим доступа: <a href="http://www.intuit.ru">http://www.intuit.ru</a></p>
Подготовка к практическому занятию Тема 3. «Основные элементы системы аттестации объектов информатизации по требованиям безопасности информации»			<p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: <a href="https://www.intuit.ru/studies/">https://www.intuit.ru/studies/</a></p>

			<p><a href="https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=">courses/3648/890/info</a></p> <p>Положение по аттестации объектов информатизации по требованиям безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL: <a href="https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=">https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=</a></p> <p>Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: <a href="https://elibrary.ru/download/elibrary_27692421_57961861.pdf">https://elibrary.ru/download/elibrary_27692421_57961861.pdf</a></p> <p>Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: <a href="https://moluch.ru/archive/52/">https://moluch.ru/archive/52/</a></p> <p>Портал ФСТЭК России - Режим доступа: <a href="http://fstec.ru">http://fstec.ru</a></p> <p>Национальный открытый университет ИНТУИТ - Режим доступа:</p>
--	--	--	--



<p>Подготовка к практическому занятию Тема 4. «Основные этапы проведения аттестации объектов информатизации»</p>			<p><a href="http://www.intuit.ru">http://www.intuit.ru</a></p> <p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: <a href="https://www.intuit.ru/studies/courses/3648/890/info">https://www.intuit.ru/studies/ courses/3648/890/info</a></p> <p>Положение по аттестации объектов информатизации по требованиям безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL: <a href="https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=">https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=</a></p> <p>Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: <a href="https://elibrary.ru/download/elibrary_27692421_57961861.pdf">https://elibrary.ru/download/ elibrary_27692421_57961861.pdf</a></p> <p>Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по</p>
--	--	--	---

			<p>требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: <a href="https://moluch.ru/archive/52/">https://moluch.ru/archive/52/</a></p> <p>Портал ФСТЭК России - Режим доступа: <a href="http://fstec.ru">http://fstec.ru</a></p> <p>Национальный открытый университет ИНТУИТ - Режим доступа: <a href="http://www.intuit.ru">http://www.intuit.ru</a></p>
--	--	--	---

## АННОТАЦИЯ

Дисциплина «Организационное обеспечение аттестации объектов информатизации» реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.

Целью дисциплины (модуля): является формирование навыков организации проведения комплекса организационно-технических мероприятий (аттестационных испытаний), в результате которых устанавливается соответствие защищаемого объекта требованиям стандартов и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Задачи: анализ функций органов аттестации, испытательных центров, заявителей и их взаимодействие при проведении аттестации объектов информатизации; изучение порядка проведения аттестации (разработка заявки на проведение аттестации, программы и методики аттестационных испытаний, их проведение), оформления и регистрации аттестата соответствия.

Дисциплина (модуль) направлена на формирование следующих компетенций:

ОПК-5 - способность использовать нормативные правовые акты в профессиональной деятельности;

ПК-5 - способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

ПК-10 - способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

ПК-15 - способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы по техническому и экспортному контролю.

В результате освоения дисциплины обучающийся должен:

знать: организацию аттестации объектов по требованиям безопасности информации; основные нормативно-правовые документы в профессиональной деятельности; виды и формы информации, подверженной угрозам; организацию проведения и сопровождения аттестацию объекта на соответствие требованиям государственных нормативных документов;

уметь: формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административной и технической реализуемости и экономической целесообразности; проводить предварительный технико-экономического анализ и обоснования проектных решений по обеспечению информационной безопасности; оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности; пользоваться нормативно-правовыми документами в области защиты информации;

владеть: способами организации и проведения (сопровождения) аттестации объекта на соответствие требованиям государственных или корпоративных нормативных документов; профессиональной терминологией; навыками использования технических средств в профессиональной деятельности; навыками работы с нормативно-правовыми.

По дисциплине (модулю) предусмотрена промежуточная аттестация в форме зачета.

Общая трудоёмкость освоения дисциплины (модуля) составляет 2 зачетные единицы.

## ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.06.2017 г.	<b>10</b>
2	<i>Обновлена основная и дополнительная литература</i>	26.06.2018 г.	<b>20</b>
3	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	26.06.2018 г.	<b>20</b>
4	<i>Обновлена основная и дополнительная литература</i>	29.08.2019 г.	<b>1</b>
5	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	29.08.2019 г.	<b>1</b>
6	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)</i>	23.06.2020 г	<b>14</b>
7	<i>Обновлена основная и дополнительная литература</i>	23.06.2020 г	<b>14</b>
8	<i>Обновлен раздел п.4 Образовательные технологии</i>	23.06.2020 г	<b>14</b>
9	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	23.06.2020 г	<b>14</b>

**1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2017 г.)**

**Перечень ПО**

*Таблица 1*

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

**Перечень БД и ИСС**

*Таблица 2*

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

д.т.н, профессор, В.В. Арутюнов

## 2. Обновление основной и дополнительной литературы (2018 г.)

В раздел 6. Учебно-методическое и информационное обеспечение дисциплины вносятся следующие изменения:

### 1. Дополнить раздел *Источники*

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/)

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_113658/](http://www.consultant.ru/document/cons_doc_LAW_113658/)

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_40241/](http://www.consultant.ru/document/cons_doc_LAW_40241/)

Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_6387/](http://www.consultant.ru/document/cons_doc_LAW_6387/)

### 2. Дополнить раздел *Основная литература*

Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с.: 60х90 1/16. - (Высшее образование) (Переплёт 7БЦ) ISBN 978-5-369-01761-6 - Режим доступа: <http://znanium.com/catalog/product/957144>

Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М. : РИОР : ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — Режим доступа: <http://znanium.com/catalog/product/937469>

Управление информационными рисками. Экономически оправданная безопасность: Пособие / Петренко С.А., Симонов С.В., - 2-е изд., (эл.) - М.:ДМК Пресс, 2018. - 396 с.: ISBN 978-5-93700-058-3 - Режим доступа: <http://znanium.com/catalog/product/983162>

## 3. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2018 г.)

### 1. Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно

			распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

#### Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

д.т.н, профессор, В.В. Арутюнов

#### 4. Обновление основной и дополнительной литературы (2019 г.)

1. В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел *Дополнительная литература*

Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — [www.dx.doi.org/10.12737/11380](http://www.dx.doi.org/10.12737/11380). - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/1009606>

#### 5. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)

##### Перечень ПО

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

##### Перечень БД и ИСС

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной



	подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

д.т.н, профессор, В.В. Арутюнов

## 6. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)

### Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 2 з. е., 76 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 48 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации ( <i>по семестрам</i> )
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Назначение и общая характеристика аттестации и сертификации в области защиты информации	7	4		2			8	опрос
2	Основные требования к защищённости базовых объектов информатизации	7	4		2			10	опрос
3	Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации	7	4		2			14	опрос
4	Порядок проведения аттестации объектов информатизации	7	4		6			16	опрос, контрольная работа
	Промежуточная аттестация								Зачет
	<b>Итого</b>		<b>16</b>		<b>12</b>			<b>48</b>	

## 7. Обновление основной и дополнительной литературы (2020 г.)

В раздел 6. Учебно-методическое и информационное обеспечение дисциплины вносятся следующие изменения:

### 1. Дополнить раздел **Дополнительная литература**

Карганов В.В. Основные положения по требованиям безопасности информации в части аттестации объектов информатизации. В сборнике: Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. Санкт-Петербург, 2020. С. 22-27. — Режим доступа: URL: [https://elibrary.ru/download/elibrary\\_43114067\\_87155282.pdf](https://elibrary.ru/download/elibrary_43114067_87155282.pdf)

Кривенцев В.А., Селифанов В.В., Звягинцева П.А. Проведение аттестационных испытаний автоматизированной системы в защищенном исполнении // Интерэкспо Гео-Сибирь. 2019. Т. 9. С. 30-34. - Режим доступа: URL: . 2019. Т. 9. С. 30-34.  
URL: [https://elibrary.ru/download/elibrary\\_41403663\\_79782082.pdf](https://elibrary.ru/download/elibrary_41403663_79782082.pdf)

8. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

9. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

#### Перечень БД и ИСС

№ п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

#### Состав программного обеспечения (ПО)

№ п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное

3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

Составитель:

д.т.н, профессор, В.В. Арутюнов