

Документ подписан простой электронной подписью  
Информация о владельце:

ФИО: Худин Александр Николаевич

Должность: Ректор

Дата подписания: 26.01.2021 12:23:18

Уникальный программный ключ:

08303ad8de1c60b987361de7085acb509ac3da145741b561afbbe37e73a19

## МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

"Курский государственный университет"

Кафедра информационной безопасности

УТВЕРЖДЕНО

протокол заседания

Ученого совета от 24.04.2017 г., №10

### Рабочая программа дисциплины Аттестация объектов информатизации

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация: бакалавр

Факультет физики, математики, информатики

Форма обучения: очная

Общая трудоемкость 4 ЗЕТ

Виды контроля в семестрах:  
экзамен(ы) 7

#### Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
	18			
Неделя	уп	рп	уп	рп
Лекции	36	36	36	36
Лабораторные	36	36	36	36
В том числе инт.	16	16	16	16
Итого ауд.	72	72	72	72
Контактная работа	72	72	72	72
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	144	144	144	144

Рабочая программа дисциплины Аттестация объектов информатизации / сост. доцент, Гордиенко В.В.;  
Курск. гос. ун-т. - Курск, 2017. - с.

Рабочая программа составлена в соответствии со стандартом, утвержденным приказом Минобрнауки России от 1 декабря 2016 г. № 1515 "Об утверждении ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата)" (Зарегистрировано в Минюсте России 20 декабря 2016 г. № 44821)

Рабочая программа дисциплины "Аттестация объектов информатизации" предназначена для методического обеспечения дисциплины основной профессиональной образовательной программы по направлению подготовки 10.03.01 Информационная безопасность профиль Безопасность компьютерных систем

Составитель(и):

доцент, Гордиенко В.В.

© Курский государственный университет, 2017

**1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

1.1	Цель(ю) изучения дисциплины является формирование знаний об организации системы государственного лицензирования в области защиты информации, сертификации и аттестации объектов защиты информации, а также организации мероприятий по информационной безопасности на объекте информатизации и об их правовом обеспечении. Дисциплина раскрывает основные понятия и виды защищаемой информации в соответствии с законодательством РФ, дает знания о системе защиты государственной тайны, конфиденциальной информации, формирует профессиональные компетенции, необходимые для осуществления профессиональной деятельности.
-----	--

**2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП**

Цикл (раздел) ООП:	Б1.В.ДВ.1
--------------------	-----------

**3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)****ОПК-1: Способностью анализировать физические явления и процессы для решения профессиональных задач****Знать:**

теоретические и методологические приёмы анализа физических явлений и процессов для решения профессиональных задач

актуальные проблемы и тенденции применения анализа физических явлений и процессов для решения профессиональных задач

основной круг проблем (задач), встречающихся в избранной сфере научной деятельности, и основные способы (методы, алгоритмы) их решения

**Уметь:**

обобщать и систематизировать передовые достижения научной мысли и основные тенденции

проводить аудит информационной безопасности предприятий, организаций вне зависимости от их формы собственности и сферы деятельности ;

определять угрозы объектов информатизации

**Владеть:**

навыками применения теоретических и методологических приёмов анализа физических явлений и процессов для решения профессиональных задач

навыками применения анализа физических явлений и процессов для решения профессиональных задач

методами решения проблем (задач), встречающихся в избранной сфере научной деятельности, и основные способы (методы, алгоритмы) их решения

**ОПК-3: Способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач****Знать:**

положения электротехники

правила применения положений электротехники ,электроники и схемотехники

специальные предупредительные знаки и их классификацию

**Уметь:**

применять положения электротехники

применять правила применения положений электротехники ,электроники и схемотехники

применять специальные предупредительные знаки и их классификацию

**Владеть:**

методами применения положений электроники

методами применения специальных предупредительные знаки и их классификацию

методами применения положений электротехники ,электроники и схемотехники

**ПК-5: Способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации****Знать:**

положение об участии в организации и сопровождении аттестации объектов информатизации

архитектуру защищённых систем

основные понятия информационной безопасности

**Уметь:**

применять методику оценки уязвимости в информационных сетях оценки

разрабатывать политику информационной безопасности на аттестуемых объектах

применять современные методы и средства защиты информации в информационно-телекоммуникационных системах

<b>Владеть:</b>
выполнять анализ корпоративных данных
методами разработки политики информационной безопасности на аттестуемых объектах
разрабатывать структуру распределения систем

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем	Вид занятий	Семестр / Курс	Часов	Интеракт.
	<b>Раздел 1. Раздел 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации</b>	Раздел			
1.1	Орган по аттестации. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации	Лек	7	4	0
1.2	Орган по аттестации. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации	Лаб	7	4	2
1.3	Орган по аттестации. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации	Ср	7	4	0
1.4	Правовой статус аттестата соответствия	Лек	7	4	2
1.5	Правовой статус аттестата соответствия	Ср	7	4	0
1.6	Правила подачи апелляции. Основные требования к содержанию	Лек	7	4	0
1.7	Правила подачи апелляции. Основные требования к содержанию	Лаб	7	4	2
1.8	Правила подачи апелляции. Основные требования к содержанию	Ср	7	4	0
1.9	Рубежный контроль	Лаб	7	2	0
	<b>Раздел 2. Раздел 2:Методические указания о порядке аттестации объектов информатизации</b>	Раздел			
2.1	Методические указания о порядке аттестации объектов информатизации по требованиям безопасности	Лек	7	4	0
2.2	Методические указания о порядке аттестации объектов информатизации по требованиям безопасности	Ср	7	4	0
2.3	Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных.	Лек	7	4	2
2.4	Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных.	Лаб	7	4	0
2.5	Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных.	Ср	7	4	0

2.6	Мероприятия по организации работ по обеспечению безопасности персональных данных. Мероприятия по обеспечению безопасности персональных данных при их обработки в системах персональных данных.	Лек	7	4	0
2.7	Мероприятия по организации работ по обеспечению безопасности персональных данных. Мероприятия по обеспечению безопасности персональных данных при их обработки в системах персональных данных.	Лаб	7	6	2
2.8	Мероприятия по организации работ по обеспечению безопасности персональных данных. Мероприятия по обеспечению безопасности персональных данных при их обработки в системах персональных данных.	Ср	7	4	0
2.9	Рубежный контроль	Лаб	7	2	0
	<b>Раздел 3. Раздел 2. Документация, сопровождающая аттестационные испытания</b>	Раздел			
3.1	Эксплуатация аттестованных объектов информатизации.	Лек	7	4	0
3.2	Эксплуатация аттестованных объектов информатизации.	Лаб	7	4	0
3.3	Эксплуатация аттестованных объектов информатизации.	Ср	7	4	0
3.4	Классификация специальных защитных знаков.	Лек	7	4	2
3.5	Классификация специальных защитных знаков.	Лаб	7	4	0
3.6	Классификация специальных защитных знаков.	Ср	7	4	0
3.7	Документация, сопровождающая аттестационные испытания	Лек	7	4	2
3.8	Документация, сопровождающая аттестационные испытания	Лаб	7	4	2
3.9	Документация, сопровождающая аттестационные испытания	Ср	7	4	0
3.10	Рубежный контроль	Лаб	7	2	0
3.11	Итоговое занятие	Экзамен	7	36	0

## 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 5.1. Контрольные вопросы и задания для текущей аттестации

Оценочные материалы для проведения текущего контроля по дисциплине "Аттестация объектов информатизации" были рассмотрены и одобрены на заседании кафедры "Программное обеспечение и администрирование информационных систем " от 30 марта 2017 г., протокол №8"

### 5.2. Фонд оценочных средств для промежуточной аттестации

Оценочные материалы для проведения промежуточной аттестации по дисциплине "Аттестация объектов информатизации" были рассмотрены и одобрены на заседании кафедры "Программное обеспечение и администрирование информационных систем " от 30 марта 2017 г., протокол №8"

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 6.1. Рекомендуемая литература

#### 6.1.1. Основная литература

	Заглавие	Эл. адрес	Кол-
--	----------	-----------	------

	Заглавие	Эл. адрес	Кол-
Л1.1	Мэйволд Э. - Безопасность сетей - Москва: Национальный Открытый Университет «ИНТУИТ», 2016.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=429035">http://biblioclub.ru/index.php?page=book&amp;id=429035</a>	1
Л1.2	Петренко В. И. - Защита персональных данных в информационных системах: учебное пособие - Ставрополь: СКФУ, 2016.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=459205">http://biblioclub.ru/index.php?page=book&amp;id=459205</a>	1
<b>6.1.2. Дополнительная литература</b>			
	Заглавие	Эл. адрес	Кол-
Л2.1	Аверченков В.И., Рыгов М.Ю. - Служба защиты информации. Организация и управление: учебное пособие - Брянск: Брянский государственный технический университет, 2012.	<a href="http://www.iprbookshop.ru/7008.html">http://www.iprbookshop.ru/7008.html</a>	1
Л2.2	В.И. Аверченков - Системы защиты информации в ведущих зарубежных странах - Москва: Флинта, 2011.	<a href="http://biblioclub.ru/index.php?page=book&amp;id=93351">http://biblioclub.ru/index.php?page=book&amp;id=93351</a>	1
<b>6.3.1 Перечень программного обеспечения</b>			
7.3.1.1	199:		
7.3.1.2	Microsoft Windows 7 (Open License: 47818817)		
7.3.1.3	Microsoft Office 2007 (OpenLicense: 43136274)		
7.3.1.4	Adobe Acrobat Reader DC (Бес-платное программное обеспечение )		
7.3.1.5	GoogleChrome (Свободная лицензия BSD)		
7.3.1.6	7-Zip (Свободная лицензия GNU LGPL),		
7.3.1.7	Visual Studio Community (Проприетарная академическая лицензия)		
7.3.1.8	СКЗИ "КриптоПроCSP" версии 4.0		
7.3.1.9	СС КонсультантПлюс (Договор № 7/ЗЦ от 14.02.2017),		
7.3.1.10	СКМ-21 ПО (Компакт-диск со специ-альным программным обеспечением)		
7.3.1.11	Смарт-ПО (Компакт-диск с про-граммным обеспечением)		
7.3.1.12	Code::Blocks (Свободная лицензия GNU GPLv3)		
7.3.1.13	EclipseNeon (Открытое программное обеспечение EclipsePublicLicense)		
7.3.1.14	USB Flash Security (Условно-бесплатное программное обеспече-ние)		
7.3.1.15	PDF Creator (Свободное программное обеспечение AGPL)		
7.3.1.16	Recuva FREE (Проприетарное услов-но-бесплатное программное обеспе-чение)		
7.3.1.17	Зоркий Глаз (Проприетарное условно-бесплатное программное обеспече-ние)		
7.3.1.18	Easy File Locker (Проприетарное ус-ловно-бесплатное программное обес-печение)		
7.3.1.19			
7.3.1.20	146:		
7.3.1.21	Microsoft Windows 7 (OpenLi-cense: 47818817)		
7.3.1.22	Ms OfficeProfessional 2007 (OpenLicense: 47818817)		
7.3.1.23	Google Chrome (Свободная ли-цензия BSD)		
7.3.1.24	7-Zip (Свободная лицензия GNU LGPL)		
7.3.1.25	Adobe Acrobat Reader DC (Бес-платное программное обеспе-чение )		
<b>6.3.2 Перечень информационных справочных систем</b>			

7.3.2.1	Каталог библиотеки КГУ. - Режим доступа: <a href="http://195.93.165.10:2280">http://195.93.165.10:2280</a>
7.3.2.2	Электронная библиотека. - Режим доступа: <a href="http://elibrary.ru">http://elibrary.ru</a>
7.3.2.3	Университетская информационная система «Россия» – <a href="http://uisrussia.msu.ru">http://uisrussia.msu.ru</a>
7.3.2.4	Электронная библиотечная система «КнигаФонд» – <a href="http://www.knigafund.ru/">http://www.knigafund.ru/</a>
7.3.2.5	Электронная библиотечная система издательства «Лань» – <a href="http://e.lanbook.com/">http://e.lanbook.com/</a>
7.3.2.6	Электронная библиотечная система «IPRbooks» – <a href="http://www.iprbookshop.ru/">http://www.iprbookshop.ru/</a>

### 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Лаборатория программно-аппаратных средств обеспечения информационной безопасности;
7.2	Лаборатория технических средств защиты информации;
7.3	для проведения занятий лекции-онного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивиду-альных консультаций, текуще-го контроля и промежуточной аттестации, самостоятельной работы,
7.4	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 199.
7.5	Моноблок LenovoC560 – 9 шт.
7.6	Стенд информационный 1,4м*0,9м – 9 шт.
7.7	Малогобаритный камуфлирован-ный блокиратор работы сотовых телефонов и закладных устройств – 1 шт.
7.8	Селективный обнаружитель циф-ровых радиоприемников ST062 – 1 шт.
7.9	Устройство защиты объектов ин-форматизации от утечки инфор-мации за счет ПЭМИН «Блокада» – 1 шт.
7.10	Нелинейный локатор «Буклет-2» – 1 шт.
7.11	Устройство МП—1А – 1 шт.
7.12	Электронно-оптическое устройст-во для обнаружения любых типов оптических устройств «Гранат» – 1 шт.
7.13	Программно-аппаратный ком-плекс «Соболь» – 1 шт.
7.14	ИМФ-3 имитатор многофункцио-нальный – 1 шт.
7.15	МониторЖК-панель 17 Асер – 1 шт.
7.16	Жалюзи вертикальные тканевые – 1 шт.
7.17	Концентратор 24порт – 1 шт.
7.18	Лабораторный комплекс «Беспро-водные сети ЭВМ»
7.19	Система активной защиты рече-вой акустической информации SEL-157 "Шагрень",
7.20	Устройство «Смарт (Комплекс оценки эффективности защиты речевой информации от утечки по акустическому, виброакустиче-скому и акустоэлектрическому каналам),
7.21	Программно-аппаратные средства защиты информации от НСД .
7.22	
7.23	Помещение для самостоятельной работы обучающихся – аудитория, оснащенная компьютерной техни-кой с возможностью подключения к сети "Интернет" и с обеспечением доступа в электронную информационно-образовательную среду университета.
7.24	305000, Курская область, г. Курск, ул. Радищева, д. № 33, 146.
7.25	Столов – 61
7.26	Посадочных мест – 162
7.27	Компьютеров:
7.28	Для пользователей – 40
7.29	Для библиотекаря – 2
7.30	Моноблоков MSI (27 ) - модель MS-A912, 2гб оперативной памяти, Athlon CPU D525 1.80GHz
7.31	Моноблоков Asus (13) - модель ET2220I, 4гб оперативной памяти, Intel Core i3-3220 CPU 3.30 GHz

### 8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Планирование и организация времени, необходимого для изучения дисциплины.  
Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:  
Изучение конспекта лекции в тот же день, после лекции - 10-15 минут.  
Изучение конспекта лекции за день перед следующей лекцией - 10-15 минут.  
Изучение теоретического материала по учебнику и конспекту - 1 час в неделю.  
Подготовка к лабораторному занятию - 30 мин.  
Всего в неделю - 2 часа 55 минут.
2. Описание последовательности действий студента («сценарий изучения дисциплины»).  
При изучении дисциплины очень полезно самостоятельно изучать материал, который еще не прочитан на лекции. Тогда

лекция будет гораздо понятнее. Однако легче при изучении курса следовать изложению материала на лекции. Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2. При подготовке к лекции следующего дня, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции (10-15 минут).

3. В течение недели выбрать время (1 час) для работы с литературой по криптографическим методам в библиотеке или изучить дополнительную литературу в электронной форме.

3. Методические рекомендации по подготовке семинарских и лабораторных занятий.

По данному курсу предусмотрены лабораторные занятия. При подготовке к лабораторным занятиям следует изучить соответствующий теоретический материал.

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по криптоанализу. Литературу по курсу «Аттестация объектов информатизации» рекомендуется изучать в библиотеке. Полезно использовать несколько учебников по курсу «Аттестация объектов информатизации». Однако легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, какие математические принципы используются в этом параграфе и каков их смысл «своими словами»? Сами криптографические протоколы следует не заучивать, а «понять». С этой целью рекомендуется записать идею протокола, составить план преобразования открытого текста в шифртекст и обратно, сравнить используемые алгоритмы и теоремы в конспекте и в учебнике. При изучении теоретического материала всегда нужно рисовать схемы или графики.

4. Рекомендации по работе с литературой.

5. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по криптографии и криптоанализу. Литературу по курсу рекомендуется изучать в библиотеке. Полезно использовать несколько учебников по изучаемому курсу. Однако легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, какие математические принципы используются в этом параграфе и каков их смысл «своими словами»? Сами криптографические протоколы следует не заучивать, а «понять». С этой целью рекомендуется записать идею протокола, составить план преобразования открытого текста в шифртекст и обратно, сравнить используемые алгоритмы и теоремы в конспекте и в учебнике. При изучении теоретического материала всегда нужно рисовать схемы или графики.