

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«Астраханский государственный университет имени В. Н. Татищева»  
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО

Руководитель ОПОП  
О.Н. Выборнова  
«04» апреля 2024 г.

УТВЕРЖДАЮ

И.о. заведующего кафедрой  
информационной безопасности  
Т.Г. Гурская  
«04» апреля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Аттестация объектов информатизации**

*наименование*

Составитель(-и)

**Шукралиева Д.Э., доцент кафедры ИБ;  
Корякова В.А., ассистент кафедры  
информационных технологий, начальник отдела  
информационной  
безопасности**

Согласовано с работодателями

**Давидюк Н.В., доцент, кандидат технических  
наук, заведующий кафедрой «Информационная  
безопасность» ФГБОУ ВО «Астраханский  
государственный технический университет»;  
Барсуков В.А., начальник отдела  
информационной безопасности Управления  
корпоративной защиты ООО «Газпром добыча  
Астрахань»**

Направление подготовки

**10.03.01 Информационная безопасность**

Направленность (профиль) ОПОП

**«Организация и технология защиты  
информации(в сфере информационных и  
коммуникационных технологий)»**

Квалификация (степень)

**бакалавр**

Форма обучения

**Очная, очно-заочная**

Год приема

**2024**

Курс

**4(по очной форме);**

Семестр(ы)

**5(по очно-заочной форме)**

**8(по очной форме);**

**9(по очно-заочной форме)**

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

**1.1. Целью освоения дисциплины (модуля) «Аттестация объектов информатизации»** является формирование у студентов представления и знаний об основных подходах и методах защиты информационных процессов в компьютерных системах, возникающих при обработке, хранении и передаче информации.

### 1.2. Задачи освоения дисциплины (модуля):

- рассмотреть основные подходы участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации,
- изучить профессиональную терминологию, законодательные акты, нормативно-методические документы по аттестации.
- сформировать умение планировать, организовывать, координировать процессы, связанные аттестацией объектов при разработке систем информационной безопасности.
- овладеть навыками разработки организационно-методического обеспечения процессов аттестации объектов на соответствие требованиям государственных или корпоративных нормативных документов.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

- Нормативные документы в области защиты информации;
- Регламенты проверок объектов информатизации по требованиям нормативных документов;
- Требования к объектам информатизации;
- Правила разработки и построения объектов информатизации.

Уметь:

- Разрабатывать проект защиты объекта информатизации;
- Доказывать корректность используемых методов защиты.

Владеть:

- Методами построения модели угроз;
- Методами аттестации объектов информатизации;
- Методами проверки;
- Средствами анализа защищенности объекта информатизации.

Бакалавр, изучив дисциплину «Аттестация объектов информатизации», может быть готов к следующему виду профессиональной деятельности:

эксплуатационная деятельность:

Бакалавр, изучив дисциплину «Аттестация объектов информатизации», должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

- участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации.

## 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

**2.1. Учебная дисциплина (модуль) Б1.Б.34 «Аттестация объектов информатизации»** входит в базовую часть учебного плана приема 2024 года набора направления подготовки 10.03.01 Информационная безопасность. Дисциплина изучается в 8 семестре, форма контроля –зачет.

**2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):**

1. Информатика.
2. Организационное и правовое обеспечение информационной безопасности.
3. Производственная практика.

В результате освоения этих дисциплин, студент должен:

**Знать:** основные понятия информатики, структуру систем документационного обеспечения.

**Уметь:** использовать программные и аппаратные средства персонального компьютера, пользоваться нормативными документами по защите информации.

**Владеть:** навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.): методикой и техникой составления различных управленческих и документов учреждений, организаций и предприятий.

**2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):**

Дисциплина «Аттестация объектов информатизации» поможет студентам при реализации задач преддипломной практики и написанию бакалаврской работы.

### **3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Процесс освоения дисциплины (модуля) направлен на формирование элементов следующей(их) компетенции(ий) в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) **общепрофессиональных (ОПК):** ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба, ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами.

**Таблица 1. Декомпозиция результатов обучения**

Код компетенции	Код и наименование индикатора достижения компетенции <sup>1</sup>	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
ОПК-2.1	ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его	ОПК-2.1.1. Знать: возможные источники информационных угроз, их возможные цели,	ОПК-2.1.2. Уметь: проводить анализ функционального процесса объекта защиты и его	ОПК-2.1.3. Владеть: методами анализа функционального процесса объекта

Код компетенции	Код и наименование индикатора достижения компетенции <sup>1</sup>	Планируемые результаты обучения по дисциплине (модулю)		
		Знать (1)	Уметь (2)	Владеть (3)
	информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	пути реализации и предполагаемый ущерб.	информационных составляющих.	защиты и его информационных составляющих.
ОПК-2.4	ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ОПК-2.4.1. Знать: нормативные документы и особенности проведения аудита защищенности объекта информатизации	ОПК-2.4.2. Уметь: проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ОПК-2.4.3. Владеть: методикой проведения аудита защищенности объекта информатизации

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

Общая трудоемкость дисциплины в соответствии с учебным планом составляет 3 зачетные единицы (108 часа).

Трудоемкость отдельных видов учебной работы студентов очной и очно-заочной формы обучения приведена в таблице 2.1.

**Таблица 2.1. Трудоемкость отдельных видов учебной работы по формам обучения**

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения
Объем дисциплины в зачетных единицах	3	3
Объем дисциплины в академических часах	108	108
Контактная работа обучающихся с преподавателем (всего), в том числе (час.):	36	27
- занятия лекционного типа, в том числе:	9	9
- практическая подготовка (если предусмотрена)		
- занятия семинарского типа (семинары, практические, лабораторные), в том числе:	27	18

Вид учебной и внеучебной работы	для очной формы обучения	для очно-заочной формы обучения
- практическая подготовка (если предусмотрена)		
- в ходе подготовки и защиты курсовой работы		
- консультация (предэкзаменационная)		
- промежуточная аттестация по дисциплине		
Самостоятельная работа обучающихся (час.)	72	81
Форма промежуточной аттестации обучающегося (зачет/экзамен), семестр (ы)	зачет – 8 семестр;	зачет – 9 семестр;

Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий и самостоятельной работы, для каждой формы обучения представлено в таблице 2.2.

**Таблица 2.2. Структура и содержание дисциплины (модуля)**

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости и, форма промежуточной аттестации
	Л		ПЗ		ЛР		КР / КП			
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП				
<i>Тема 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.</i>	2				8			16	26	<i>Контрольная работа 1.</i>
<i>Тема 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации</i>	2				8			16	26	<i>Контрольная работа 2.</i>
<i>Тема 3. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных</i>	2				4			14	20	<i>отчет по лабораторной работе 1.</i>
<i>Тема 4. Оформление результатов аттестационных испытаний</i>	2				4			14	20	<i>отчет по лабораторной работе 2</i>
<i>Тема 5. Эксплуатация аттестованных объектов информатизации</i>	1				3			12	16	<i>Контрольная работа 3.</i>
<b>Консультации</b>										
<b>Контроль промежуточной аттестации</b>										<b>Зачёт</b>
<b>ИТОГО за семестр:</b>	<b>9</b>				<b>27</b>			<b>72</b>	<b>108</b>	

**для очно-заочной формы обучения**

Раздел, тема дисциплины (модуля)	Контактная работа, час.							СР, час.	Итого часов	Форма текущего контроля успеваемости и, форма промежуточ ной аттестации
	Л	в т.ч. ПП	ПЗ	в т.ч. ПП	ЛР	в т.ч. ПП	КР / КП			
<i>Тема 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.</i>	2				6			18	26	<i>Контрольная работа 1.</i>
<i>Тема 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации</i>	2				6			18	26	<i>Контрольная работа 2.</i>
<i>Тема 3. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных</i>	2				2			16	20	<i>отчет по лабораторной работе 1.</i>
<i>Тема 4. Оформление результатов аттестационных испытаний</i>	2				2			16	20	<i>отчет по лабораторной работе 2</i>
<i>Тема 5. Эксплуатация аттестованных объектов информатизации</i>	1				2			13	16	<i>Контрольная работа 3.</i>
<b>Консультации</b>										
<b>Контроль промежуточной аттестации</b>										<b>Зачёт</b>
<b>ИТОГО за семестр:</b>	<b>9</b>				<b>18</b>			<b>81</b>	<b>108</b>	

*Примечание:* Л – лекция; ПЗ – практическое занятие, семинар; ЛР – лабораторная работа; ПП – практическая подготовка; КР / КП – курсовая работа / курсовой проект; СР – самостоятельная работа

**Таблица 3. Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций**

Раздел, тема дисциплины (модуля)	Кол-во часов	Код компетенции		Общее количество компетенций
		ОПК-2.1	ОПК-2.4	
Тема 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.	26	+	+	2
Тема 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации	26	+	+	2
Тема 3. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных	20	+	+	2
Тема 4. Оформление результатов аттестационных испытаний	20	+	+	2
Тема 5. Эксплуатация аттестованных объектов информатизации	16	+	+	2
<b>ИТОГО</b>	<b>108</b>			

### Содержание дисциплины (модуля)

#### **Тема 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.**

Орган по аттестации. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации. Правовой статус аттестата соответствия. Подача апелляции

#### **Тема 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации**

Анализ исходных данных по аттестуемому объекту информатизации; предварительное ознакомление с аттестуемым объектом информатизации. Проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации. Проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств; проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям

безопасности информации. Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации. Анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

### **Тема 3. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных**

Общие положения. Подготовительный этап.

Мероприятия по организации работ по обеспечению безопасности персональных данных

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации.

Контроль и надзор за эксплуатацией аттестованных информационных систем персональных данных. Ответственность оператора за нарушение правил обращения с персональными данными

### **Тема 4. Оформление результатов аттестационных испытаний**

Заявка на проведение аттестации объекта информатизации

Аттестат соответствия требованиям безопасности информации

Типовая форма акта классификации

Типовая форма матрицы доступа

Рекомендуемые формы приказов

Инструкция по учету лиц

Рекомендуемая форма модели угроз

Типовая форма требований по обеспечению безопасности персональных данных

Типовая форма журнала учета средств защиты информации

Типовая форма заключения о возможности эксплуатации средств защиты информации

Типовая форма инструкции по организации резервирования

Типовая форма журнала учета машинных носителей

Типовая форма акта обследования

Типовая форма заключения по результатам аттестационных испытаний

Типовая форма описания системы защиты

Типовая форма аттестата соответствия

Перечень вопросов по обеспечению безопасности персональных данных

### **Тема 5. Эксплуатация аттестованных объектов информатизации**

Переаттестация. Ответственность владельца аттестованного объекта информатизации. Действия в случае изменения условий и технологий обработки защищаемой информации. Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации. Приостановление или аннулирование действие аттестата соответствия.

## **5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

### **5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)**

**Методические рекомендации по выполнению лабораторных и контрольных работ, проведению зачета**

### Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной лабораторной работе должны быть указаны:

- тема лабораторной работы,
- пакет документов в соответствии с темой лабораторной работы,
- использованная литература.

### Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретических заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Оценивание студентов на зачете осуществляется в соответствии с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе экзамена.

На учебном файловом сервере АГУ (fsever) размещены задания для лабораторной и самостоятельной работы студентов, тесты, а также лекционный материал.

## 5.2. Указания для обучающихся по освоению дисциплины (модулю)

Таблица 4. Содержание самостоятельной работы обучающихся

*для очной формы обучения*

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
<i>Тема 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.</i>	16	Контрольная работа 1.
<i>Тема 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации</i>	16	Контрольная работа 2.
<i>Тема 3. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных</i>	14	Отчет по лабораторной работе 1.

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
<i>данных</i>		
<i>Тема 4. Оформление результатов аттестационных испытаний</i>	14	Отчет по лабораторной работе 2.
<i>Тема 5. Эксплуатация аттестованных объектов информатизации</i>	12	Контрольная работа 3.

**для очно-заочной формы обучения**

Вопросы, выносимые на самостоятельное изучение	Кол-во часов	Форма работы
<i>Тема 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.</i>	18	Контрольная работа 1.
<i>Тема 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации</i>	18	Контрольная работа 2.
<i>Тема 3. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных</i>	16	Отчет по лабораторной работе 1.
<i>Тема 4. Оформление результатов аттестационных испытаний</i>	16	Отчет по лабораторной работе 2.
<i>Тема 5. Эксплуатация аттестованных объектов информатизации</i>	13	Контрольная работа 3.

**5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины (модуля), выполняемые обучающимися самостоятельно**

**Темы для самостоятельной работы**

1. Сертификация программных продуктов – Common Criteria
2. Особенности аттестации объектов информатизации по требованиям безопасности речевой информации
3. Требования к информационным системам персональных данных в странах западной Европы и США
4. Требования к оформлению аттестационных испытаний в странах западной Европы и США.
5. Требования к эксплуатации аттестованных объектов информатизации в странах западной Европы и США.

**6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

**6.1. Образовательные технологии**

В соответствии с требованиями ФГОС ВПО по направлению подготовки бакалавров в рамках изучения дисциплины предусмотрено использование в учебном процессе следующих активных и интерактивных форм проведения занятий

**Таблица 5. Образовательные технологии, используемые при реализации учебных занятий**

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
<i>Тема 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.</i>	<i>Обзорная лекция</i>	<i>Не предусмотрено</i>	<i>Фронтальный опрос, выполнение практических заданий, тематические дискуссии</i>
<i>Тема 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации</i>	<i>Лекция-диалог</i>	<i>Не предусмотрено</i>	<i>Тематические дискуссии, анализ конкретных ситуаций</i>
<i>Тема 3. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных</i>	<i>Лекция-диалог</i>	<i>Не предусмотрено</i>	<i>Выполнение контрольной работы</i>
<i>Тема 4. Оформление результатов аттестационных испытаний</i>	<i>Лекция-диалог</i>	<i>Не предусмотрено</i>	<i>Выполнение лабораторной работы</i>
<i>Тема 5. Эксплуатация аттестованных объектов информатизации</i>	<i>Лекция-диалог</i>	<i>Не предусмотрено</i>	<i>Выполнение лабораторной работы</i>

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных образовательных технологий не должен превышать 25%.

## **6.2. Информационные технологии**

Информационные технологии, используемые при реализации различных видов учебной и внеучебной работы:

- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;

- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные

ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

- использование виртуальной обучающей среды (или системы управления обучением LMS Moodle) или иных информационных систем, сервисов и мессенджеров.

Название информационной технологии	Темы, разделы дисциплины	Краткое описание применяемой технологии
Использование возможностей Интернета в учебном процессе	1 – 5	Проведение рейтингового контроля знаний учащихся (в системах дистанционного обучения)
Использование возможностей электронной почты преподавателя	1 – 5	Подготовка к защите отчетов по лабораторным работам
Использование средств представления учебной информации	1 – 5	Использование мультимедийной презентации

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии: виртуальная обучающая среда (или система управления обучением LMS Moodle) или иные информационные системы, сервисы и мессенджеры.

### **6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы**

#### **6.3.1. Программное обеспечение**

В соответствии с ОПОП дисциплина должна быть поддержана соответствующими лицензионными программными продуктами.

При использовании электронных изданий вуз обеспечивает каждого обучающегося рабочим местом в компьютерном классе в соответствии с объемом изучаемых дисциплин, обеспечивает выход в сеть Интернет.

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
MathCad 14	Система компьютерной алгебры из класса систем автоматизированного проектирования, ориентированная на подготовку интерактивных документов с вычислениями и визуальным сопровождением, отличается лёгкостью использования
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда

Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты
MS Visual Studio	Среда разработки программ для ЭВМ

### 6.3.2. Современные профессиональные базы данных и информационные справочные системы

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем» <https://library.asu.edu.ru>
2. Электронно-библиотечная система elibrary <http://elibrary.ru>
3. Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС» <http://dlib.eastview.com/>

## 7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

### 7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Аттестация объектов информатизации» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

**Таблица 6. Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств**

Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
Тема 1. Основные принципы, организационная структура системы аттестации объектов информатизации	<b>ОПК 2.1, ОПК 2.4</b>	Контрольная работа 1.

по требованиям безопасности информации.		
Тема 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации	<i>ОПК 2.1, ОПК 2.4</i>	Контрольная работа 2.
Тема 3. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных	<i>ОПК 2.1, ОПК 2.4</i>	отчет по лабораторной работе 1.
Тема 4. Оформление результатов аттестационных испытаний	<i>ОПК 2.1, ОПК 2.4</i>	отчет по лабораторной работе 2
Тема 5. Эксплуатация аттестованных объектов информатизации	<i>ОПК 2.1, ОПК 2.4</i>	Контрольная работа 3.

## 7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

**Таблица 7. Показатели оценивания результатов обучения в виде знаний**

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

**Таблица 8. Показатели оценивания результатов обучения в виде умений и владений**

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы

Шкала оценивания	Критерии оценивания
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание по подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задания

### 7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

#### Тема 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.

##### Вопросы к контрольной работе № 1

1. Орган по аттестации.
2. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.
3. Правовой статус аттестата соответствия.
4. Подача апелляции
5. Анализ исходных данных по аттестуемому объекту информатизации; предварительное ознакомление с аттестуемым объектом информатизации.
6. Проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации.
7. Проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств.
8. Проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации.
9. Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации.
10. Анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

#### Тема 2. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации.

##### Вопросы к контрольной работе №2

1. Мероприятия по организации работ по обеспечению безопасности персональных данных
2. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

3. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации.

4. Контроль и надзор за эксплуатацией аттестованных информационных систем персональных данных. Ответственность оператора за нарушение правил обращения с персональными данными

5. Заявка на проведение аттестации объекта информатизации. Аттестат соответствия требованиям безопасности информации

6. Типовая форма акта классификации. Типовая форма матрицы доступа

7. Рекомендуемые формы приказов. Инструкция по учету лиц.

8. Рекомендуемая форма модели угроз.

### **Тема 3. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных.**

#### **Лабораторно-практическая работа 1. Разработка политики безопасности.**

Цель работы: изучение принципов совокупности норм и правил, определяющих принятые в организации меры по обеспечению безопасности информации, связанной с деятельностью организации.

Задача №1: Выбрать организацию, обрабатывающую конфиденциальную информацию, изучить какую информацию в ней обрабатывают, объем информации, потоки данных.

Задача №2: Разработать документ, определяющий политику безопасности в данной организации.

#### **Тема 4. Оформление результатов аттестационных испытаний.**

##### **Лабораторно-практическая работа 2. Проведение аттестационных испытаний**

##### **компьютерных систем в защищенном исполнении и выдача «Аттестата соответствия».**

Цель работы: изучение порядка проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

Задача №1: Выбрать информационную систему персональных данных для организации, рассмотренной в лабораторной работе 1.

Задача №2: Разработать пакет документов, необходимый для получения аттестата соответствия данной системы.

#### **Тема 5. Эксплуатация аттестованных объектов информатизации.**

##### **Вопросы к контрольной работе №3**

1. Типовая форма требований по обеспечению безопасности персональных данных

2. Типовая форма журнала учета средств защиты информации.

3. Типовая форма заключения о возможности эксплуатации средств защиты информации.

4. Типовая форма инструкции по организации резервирования.

5. Типовая форма журнала учета машинных носителей.

6. Типовая форма акта обследования.

7. Типовая форма заключения по результатам аттестационных испытаний.

8. Типовая форма описания системы защиты.

9. Типовая форма аттестата соответствия.

10. Перечень вопросов по обеспечению безопасности персональных данных.

11. Переаттестация.

12. Ответственность владельца аттестованного объекта информатизации.

13. Действия в случае изменения условий и технологий обработки защищаемой информации.

14. Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации.
15. Приостановление или аннулирование действие аттестата соответствия.

**Примерный перечень вопросов к зачету по дисциплине  
«Аттестация объектов информатизации»**

1. Орган по аттестации.
2. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.
3. Правовой статус аттестата соответствия. Подача апелляции
4. Анализ исходных данных по аттестуемому объекту информатизации
5. предварительное ознакомление с аттестуемым объектом информатизации
6. Проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации.
7. Проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств проведения испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации.
8. Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации.
9. Анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.
10. Подготовительный этап. Мероприятия по организации работ по обеспечению безопасности персональных данных
11. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
12. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации
13. Контроль и надзор за эксплуатацией аттестованных информационных систем персональных данных
14. Ответственность оператора за нарушение правил обращения с персональными данными
15. Оформление заявки на проведение аттестации объекта информатизации
16. Содержание типовой формы Аттестат соответствия требованиям безопасности информации
17. Содержание типовой формы акта классификации
18. Содержание типовой формы матрицы доступа
19. Рекомендуемые формы приказов
20. Инструкция по учету лиц
21. Рекомендуемая форма модели угроз
22. Содержание типовой формы требований по обеспечению безопасности персональных данных
23. Содержание типовой формы журнала учета средств защиты информации
24. Содержание типовой формы заключения о возможности эксплуатации средств защиты информации
25. Содержание типовой формы инструкции по организации резервирования
26. Содержание типовой формы журнала учета машинных носителей
27. Содержание типовой формы акта обследования

28. Содержание типовой формы заключения по результатам аттестационных испытаний  
 29. Содержание типовой формы описания системы защиты  
 30. Содержание типовой формы аттестата соответствия  
 31. Перечень вопросов по обеспечению безопасности персональных данных  
 32. Переаттестация.  
 33. Ответственность владельца аттестованного объекта информатизации.  
 34. Действия в случае изменения условий и технологий обработки защищаемой информации.  
 35. Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации.  
 36. Приостановление или аннулирование действие аттестата соответствия.

**Таблица 9. Примеры оценочных средств с ключами правильных ответов**

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ОПК-2.1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба				
1.	Задание закрытого типа	Совокупность органов и (или) исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации 1) Система защиты информации 2) Способ защиты информации 3) Метод защиты информации 4) Регламентация защиты информации	1	3
2.		Какие степени секретности для составления документации установлены Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»? 1.Секретно 2.Для служебного пользования 3.Совершенно секретно 4.Особой важности 5.Конфиденциально 6.Анонимно	1, 3, 4	2
3.		Какие из предложенных сведений не подлежат засекречиванию в соответствии	2, 3, 5	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		<p>с Законом Российской Федерации «О государственной тайне»?</p> <ol style="list-style-type: none"> <li>1.Сведения о сущности изобретения до официальной публикации о них</li> <li>2.Сведения о состоянии здоровья высших должностных лиц России</li> <li>3.Сведения о фактах нарушения прав и свобод человека</li> <li>4.Сведения, составляющие тайну следствия и судопроизводства</li> <li>5.Сведения о состоянии преступности</li> </ol>		
4.		<p>Система безопасности - это ...?</p> <ol style="list-style-type: none"> <li>1. организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно-важных интересов личности, предприятия, государства от внутренних и внешних угроз</li> <li>2. защищенность информации от случайных или преднамеренных воздействий искусственного или естественного характера, способных нанести неприемлемый ущерб субъектам информационных отношений</li> <li>3. специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообуславливающих друг друга сторон, свойств, тенденций</li> </ol>	1	2
5.		<p>Процедура оформления права сотрудника или иного лица на доступ к сведениям ограниченного распространения и одновременно правовой акт согласия собственника</p>	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		<p>информации на передачу ее для работы конкретному лицу - это ...?</p> <ol style="list-style-type: none"> <li>1. допуск</li> <li>2. доступ</li> <li>3. режим</li> <li>4. аттестация</li> </ol>		
6.	Задание открытого типа	Какие реквизиты наносятся на носители сведений, составляющих государственную тайну	<p>На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:</p> <ul style="list-style-type: none"> <li>• о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;</li> <li>• об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;</li> <li>• о регистрационном номере;</li> <li>• о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.</li> </ul>	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
7.		Органы защиты государственной тайны	<p>К органам защиты государственной тайны относятся:</p> <ul style="list-style-type: none"> <li>• межведомственная комиссия по защите государственной тайны;</li> <li>• органы федеральной исполнительной власти: ФСБ, МО, СВР, ФСТЭК;</li> <li>• органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.</li> </ul>	7
8.		Что предусматривает допуск должностных лиц и граждан к государственной тайне	<p>Допуск должностных лиц и граждан к государственной тайне предусматривает:</p> <ol style="list-style-type: none"> <li>1. Принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну.</li> <li>2. Согласие на частичные, временные ограничения их прав в соответствии со статьей 24 закона «О государственной тайне»: <ul style="list-style-type: none"> <li>• права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска</li> </ul> </li> </ol>	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			<p>гражданина к государственной тайне;</p> <ul style="list-style-type: none"> <li>• права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;</li> <li>• права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.</li> </ul> <p>3. Письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий.</p> <p>4. Определение видов, размеров и порядка предоставления социальных гарантий, предусмотренных настоящим Законом;</p> <p>5. Ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение.</p> <p>6. Принятие решения руководителем органа государственной власти, предприятия, учреждения или</p>	

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			организации о допуске оформляемого лица к сведениям, составляющим государственную тайну	
9.		Цель проведения проверочных мероприятий	<p>Целью проведения проверочных мероприятий является выявление следующих оснований, предусмотренных статьей 22 закона «О государственной тайне»:</p> <ul style="list-style-type: none"> <li>- признание его судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;</li> <li>- наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому федеральным органом исполнительной власти, уполномоченным в области здравоохранения и социального развития;</li> <li>- постоянное проживание его самого и (или) его близких</li> </ul>	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			<p>родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;</p> <ul style="list-style-type: none"> <li>- выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;</li> <li>- уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.</li> </ul>	
10.		<p>При выполнении каких условий обеспечивается эффективная защита предприятия?</p>	<p>Эффективная защита предприятия обеспечивается при выполнении следующих условий:</p> <ul style="list-style-type: none"> <li>- единство в решении производственных, коммерческих, финансовых и режимных вопросов;</li> <li>- координация мер безопасности между заинтересованными подразделениями фирмы;</li> <li>- разработка режимных мер на основе оценки информации и объектов, подлежащих защите (классификации);</li> <li>- персональная ответственность на всех исполнительских уровнях за обеспечение</li> </ul>	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			<p>сохранности конфиденциальной информации;</p> <ul style="list-style-type: none"> <li>- организация специального делопроизводства, введение соответствующей маркировки документов;</li> <li>- разработка и утверждение списка с перечнем лиц, допущенным к такого рода информации;</li> <li>- наличие охраны, а также пропускного и внутриобъектового режимов.</li> </ul>	
ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами				
1.	Задание закрытого типа	<p>Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации:</p> <ol style="list-style-type: none"> <li>1. Защита информации от несанкционированного доступа</li> <li>2. Защита информации от несанкционированного воздействия</li> <li>3. Защита информации от непреднамеренного воздействия</li> </ol>	1	3
2.		<p>Деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации</p> <ol style="list-style-type: none"> <li>1. Защита информации от разглашения</li> <li>2. Защита информации от утечки</li> <li>3. Защита информации от НСД</li> </ol>	1	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
3.		Отнесение сведений к государственной тайне и их засекречивание осуществляется в соответствии с какими принципами 1. законности 2. обоснованности 3. своевременности 4. комплексности 5. разумной достаточности 6. целесообразности	1, 2, 3	2
4.		Одним из факторов, усиливающим активизацию угроз безопасности предпринимательству является. 1. Установление контроля монополистических предприятий над рядом секторов экономики и субъектами хозяйственной деятельности. 2. Установление контроля криминальных структур над рядом секторов экономики и субъектами хозяйственной деятельности. 3. Установление контроля властных структур над субъектами хозяйственной деятельности.	2	2
5.		Недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации 1. Уязвимость 2. Угроза 3. Ущерб 4. Риск	1	3
6.	Задание открытого типа	Требования к руководителю для проведения государственной аттестации ?	Для проведения государственной аттестации руководителю необходимо: 1) Знать руководящие и регламентирующие документы в области защиты	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			государственной тайны, уметь ими пользоваться и руководствоваться в организации мероприятий по ЗГТ. 2) Иметь действующий допуск к государственной тайне.	
7.		Какие объекты информатизации подлежат обязательной аттестации?	Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров.	5
8.		Аттестации объектов информатизации по требованиям безопасности информации проводится в несколько этапов:	Аттестации объектов информатизации по требованиям безопасности информации проводится в несколько этапов: 1. Подача и рассмотрение заявки на аттестацию. 2. Анализ исходных данных по аттестуемому объекту информатизации. 3. Предварительное ознакомление с аттестуемым объектом информатизации. 4. Испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости).	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			<p>5. Разработка программы и методики аттестационных испытаний.</p> <p>6. Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации.</p> <p>7. Выдача "Аттестата соответствия".</p>	
9.		<p>Какие исходные данные и документацию представляет заявитель органу по аттестации для проведения испытаний?</p>	<p>Для проведения испытаний заявитель представляет органу по аттестации следующие исходные данные и документацию: - приемо-сдаточную документацию на объект информатизации; - акты категорирования выделенных помещений и объектов информатизации; - инструкции по эксплуатации средств защиты информации; - технический паспорт на аттестуемый объект; - документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ; - сертификаты соответствия требованиям безопасности информации на ВТСС; - сертификаты соответствия требованиям безопасности информации на</p>	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			<p>технические средства защиты информации; - акты на проведенные скрытые работы; - протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились); - протоколы измерения величины сопротивления заземления; - протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки; - данные по уровню подготовки кадров, обеспечивающих защиту информации; - данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке; - нормативную и методическую документацию по защите информации и контролю эффективности защиты.</p>	
10.		<p>Какие объекты подлежат специальным проверкам на наличие возможно внедренных специальных электронных устройств перехвата информации?</p>	<p>Специальным проверкам на наличие возможно внедренных специальных электронных устройств перехвата информации подлежат: -</p>	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			выделенные помещения, предназначенные для проведения закрытых мероприятий; - технические средства, предназначенные для обработки информации ограниченного доступа; - вспомогательные технические средства, устанавливаемые в выделенных помещениях и на объектах информатизации.	

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

#### **7.4. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)**

##### **Критерии оценки зачета:**

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по основам ИБ.

**Таблица 10. Технологическая карта рейтинговых баллов по дисциплине (модулю)**

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
<b>Основной блок</b>				
1.	<i>Ответ на занятии</i>	5/10	25	В течение семестра

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
2.	<i>Выполнение лабораторной работы</i>	2/10	20	В течение семестра
3.	<i>Выполнение контрольной работы</i>	3/15	45	В течение семестра
<b>Всего</b>			<b>90</b>	-
<b>Блок бонусов</b>				
4.	<i>Посещение занятий</i>	5	1	В течение семестра
5.	<i>Своевременное выполнение всех заданий</i>	5	1	В течение семестра
<b>Всего</b>			<b>10</b>	-
<b>ИТОГО</b>			<b>100</b>	-

**Таблица 11. Система штрафов (для одного занятия)**

Показатель	Балл
<i>Опоздание на занятие</i>	-1
<i>Нарушение учебной дисциплины</i>	-1
<i>Неготовность к занятию</i>	-10
<i>Пропуск занятия без уважительной причины</i>	-5

**Таблица 12. Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)**

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

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

### 8.1. Основная литература

1. "Защита информации от несанкционированного доступа: метод. указания к выполнению лабораторной работы по курсу "Аттестация объектов информатизации" [Электронный ресурс] / А.А. Герасимов, А.В. Мозговой. - М. : Издательство МГТУ им. Н. Э. Баумана, 2012." - [http://www.studentlibrary.ru/book/bauman\\_0485.html](http://www.studentlibrary.ru/book/bauman_0485.html)
2. Оценка состояния организационных систем: принципы, модели, технология [Электронный ресурс] / Я.П. Демидов, Н.Г. Багаутдинова, Л.Б. Шабанова - Казань : Изд-во Казан. ун-та, 2016. - <http://www.studentlibrary.ru/book/ISBN9785000196151.html>

### 8.2. Дополнительная литература

1. Правовой режим лицензирования и сертификации в сфере информационной безопасности [Электронный ресурс] : Учебное пособие / Коваленко Ю.И. - М. : Горячая линия - Телеком, 2012. - <http://www.studentlibrary.ru/book/ISBN9785991202619.html>

### **8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)**

1. Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. [www.studentlibrary.ru](http://www.studentlibrary.ru).

## **9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Учебные аудитории, библиотеки АГУ, компьютерные классы, мультимедийные аудитории.

Материально-техническое обеспечение дисциплины включает в себя учебные лаборатории и классы, оснащенные современными компьютерами, объединенными локальными вычислительными сетями с выходом в Интернет. Учащимся предоставляется возможность практической работы на ЭВМ различной архитектуры (на базе одноядерных, многоядерных, параллельных процессоров).

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

## **10. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ**

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т. д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при

этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т. д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).