МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГАОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность
Код и наименование направления подготовки/специальности

Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2026

Организационное обеспечение аттестации объектов информатизации
Рабочая программа дисциплины

Составитель(и):
Кандидат венных наук, доцент кафедры КЗИ Д.Н. Баранников

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 5 от 25.12.2025

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – 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, утверждённых ФСТЭК России.

Задачи дисциплины:

- 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:

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-5 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	*ПК-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации*	*Знать:* - *нормативные правовые акты, методические документы, национальные стандарты в области аттестации объектов информатизации на соответствие требованиям по защите информации;*
	ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации	*Уметь:* - *разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации,* - *проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации;*
	ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений	*Владеть:* - *способами организации и проведения (сопровождения) аттестации объекта на соответствие требованиям*

	требованиям по защите информации	*государственных или корпоративных нормативных документов; профессиональной терминологией; навыками использования технических средств в профессиональной деятельности; навыками составления необходимых документов при проведении аттестации объектов информатизации*
ПК-10 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	*ПК-10.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации*	*Знать: нормативные правовые акты, методические документы, национальные стандарты в области аттестации объектов информатизации на соответствие требованиям по защите информации;*
	ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации	*Уметь: разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации;*
	ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	*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*

		составления необходимых документов при проведении аттестации объектов информатизации
ПК-15 Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	*ПК-15.1 Знает технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами*	*Знать: нормативные правовые акты, методические документы, национальные стандарты в области аттестации объектов информатизации на соответствие требованиям по защите информации;*
	ПК-15.2 Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке	*Уметь: разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации;*
	ПК-15.3 Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся 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 составления необходимых документов при проведении аттестации объектов информатизации;*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Организационное обеспечение аттестации объектов информатизации» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _3_ з.е., _108__ академических часа.

Структура дисциплины для очной формы обучения

Семестр	Тип учебных занятий	Количество часов
5	Лекции	26
5	Практические работы	28
Всего:		54

Объем дисциплины в форме самостоятельной работы обучающихся составляет 54 академических часа.

3. Содержание дисциплины

Тема 1. Правовые основы аттестации объектов информатизации

Понятийный аппарат в области аттестации объектов информатизации. Виды информации. Правовые основы аттестации объектов информатизации. Связь с мероприятиями по специсследованиям, спецобследованиям и спецпроверкам объектов информатизации.

Тема 2 Место и роль аттестации объектов информатизации в системе защиты информации

Цель аттестации. Общие требования к организации аттестации объектов информатизации. Обязательная аттестация. Добровольная аттестация. Объекты информатизации. Объекты, подлежащие обязательной аттестации.

Тема 3. Структура системы аттестации объектов информатизации

Основные составляющие структуры аттестации объектов информатизации.

Федеральный орган по сертификации средств защиты и аттестации объектов информатизации по требованиям безопасности информации, его функции.

Органы по аттестации объектов. Требования к органу по аттестации объектов информатизации по требованиям безопасности информации, лицензирование его деятельности предприятий в качестве испытательных центров. Задачи и функции органа по аттестации. Деятельность аттестационных комиссий. Права, обязанности и ответственность органа по аттестации.

Аккредитация испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информацию. Общие требования. Порядок аккредитации предприятия. Контроль и надзор за деятельностью аккредитованных испытательных лабораторий и органов по сертификации. Аннулирование аккредитации предприятий в качестве испытательных лабораторий и органов по сертификации.

Заявители-заказчики, владельцы, разработчики аттестуемых объектов информатизации. Требования к деятельности заявителей. Заявка на проведение аттестации объекта информатизации-аттестационных испытаний автоматизированной системы или аттестационных испытаний выделенного помещения. Порядок представления исходных данных по аттестуемому объекту информатизации. Требования на подготовку объекта информатизации к его аттестации, предоставления органам по аттестации необходимые документы, осуществления эксплуатации объекта в соответствии с требованиями, установленными в «Аттестате соответствия».

Тема 4. Порядок проведения аттестации объекта информатизации

Подготовительный этап. Подача и рассмотрение заявки на аттестацию объекта. Предварительное ознакомление с аттестуемым объектом. Испытание несертифицированных средств и систем защиты информации. Разработка программы и методики аттестационных испытаний. Заключение договора на проведение аттестации.

Основной этап. Проведение аттестационных испытаний объекта информатизации. Оформление протоколов испытаний и заключения.

Заключительный этап. Оформление, регистрация и выдача «Аттестата соответствия».

Тема 5. Порядок проведения аттестационных испытаний защищаемого помещения

Проверка выполнения требований по защите информации от утечки за счёт ПЭМИН. Проверка эффективности работы средств и систем акустической и виброакустической защиты, систем активной защиты соединительных линий ВТСС, линий электропитания и заземления. Выявление специальных электронных устройств перехвата информации—спецобследования защищаемого помещения и спецпроверка наличия закладных устройств в технических средствах защищаемого помещения. Технические средства необходимые для проведения аттестации защищаемых помещений.

Тема 6. Порядок проведения аттестационных испытаний автоматизированной системы.

Проверка соответствия исходных данных реальным условиям эксплуатации, проверка АС на соответствие организационно-техническим требованиям по защите информации. Проверка выполнения требований от утечки за счёт наводок на ВТСС. Проверка выполнения требований от утечки по цепям электропитания и заземления. Проверка выполнения требований на отсутствие закладочных устройств в автоматизированной системе. Организация испытаний на соответствие требованиям по защите информации от НСД. Классификация АС по защите от НСД. Технические средства необходимые для проведения аттестации автоматизированной системы.

4. Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	*Правовые основы аттестации объектов информатизации*	*Лекция 1.1* *Лекция 1.2* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Изучение материалов лекций*
2	*Место и роль аттестации объектов информатизации в системе защиты информации*	*Лекция 2.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Изучение материалов лекций*
3	*Структура системы аттестации объектов информатизации*	*Лекция 3.1* *Лекция 3.2* *Практическое занятие 1.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Выполнение задания* *Изучение материалов лекций*
4	*Порядок проведения аттестации объекта информатизации*	*Лекция 4.* *Практическое занятие 1.*	*Традиционная с использованием презентаций* *Выполнение задания*

		Самостоятельная работа	*Изучение материалов лекций*
5	*Порядок проведения аттестационных испытаний защищаемого помещения*	*Лекция 5.1* *Лекция 5.2* *Практическое занятие 2.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Выполнение задания* *Изучение материалов лекций*
6	*Порядок проведения аттестационных испытаний автоматизированной системы*	*Лекция 6.1* *Лекция 6.2* *Практическое занятие 3.* *Самостоятельная работа*	*Традиционная с использованием презентаций* *Выполнение задания* *Изучение материалов лекций*

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.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1-6)* *– практическое задание 1…3*	 *5 баллов* *10 баллов*	 *30 баллов* *30 баллов*
Промежуточная аттестация – *зачёт*		40 баллов
Итого за семестр		100 баллов

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:

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	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. 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. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	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. 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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	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. 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. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Вопросы для устного опроса

№	Вопрос	Реализуемая компетенция
1.	Классификация информации в зависимости от порядка её предоставления или распространения	ПК-5; ПК-10; ПК-15
2.	Виды информации, доступ к которой должен быть ограничен	ПК-5; ПК-10; ПК-15
3.	Нормативные документы по аттестации объектов информатизации	ПК-5; ПК-10; ПК-15
4.	Что понимается под объектом информатизации и аттестацией объекта информатизации	ПК-5; ПК-10; ПК-15
5.	Определение разведдоступности	ПК-5; ПК-10; ПК-15
6.	Определение специальных проверок, специального обследования и специальных исследований	ПК-5; ПК-10; ПК-15
7.	Цели аттестации ОИ.	ПК-5; ПК-10; ПК-15
8.	Виды аттестации.	ПК-5; ПК-10; ПК-15
9.	Общие требования к организации аттестации объектов информатизации.	ПК-5; ПК-10; ПК-15
10.	Обязательная аттестация.	ПК-5; ПК-10; ПК-15
11.	Добровольная аттестация.	ПК-5; ПК-10; ПК-15
12.	Объекты, подлежащие обязательной аттестации.	ПК-5; ПК-10; ПК-15
13.	Основные составляющие структуры аттестации объектов информатизации	ПК-5; ПК-10; ПК-15
14.	Органы по аттестации объектов.	ПК-5; ПК-10; ПК-15
15.	Требования к органу по аттестации объектов информатизации по требованиям безопасности информации,	ПК-5; ПК-10; ПК-15
16.	Лицензирование деятельности предприятий в качестве испытательных центров.	ПК-5; ПК-10; ПК-15
17.	Требования к деятельности заявителей.	ПК-5; ПК-15
18.	Этапы проведения аттестации ОИ	ПК-5; ПК-10; ПК-15
19.	Испытание несертифицированных средств и систем защиты информации.	ПК-5; ПК-15
20.	Разработка программы и методики аттестационных испытаний.	ПК-5;
21.	Проведение аттестационных испытаний объекта информатизации	ПК-5; ПК-10; ПК-15
22.	«Аттестат соответствия»	ПК-5; ПК-10; ПК-15
23.	Выявление специальных электронных устройств перехвата информации	ПК-5; ПК-10; ПК-15
24.	Технические средства необходимые для проведения аттестации защищаемых помещений	ПК-5; ПК-10; ПК-15
25.	Проверка выполнения требований по защите информации от утечки за счёт ПЭМИН.	ПК-5; ПК-10; ПК-15
26.	Проверка выполнения требований от утечки за счёт наводок	ПК-5; ПК-10; ПК-15

	на ВТСС.	
27.	Проверка выполнения требований от утечки по цепям электропитания и заземления.	ПК-5; ПК-10; ПК-15
28.	Классификация АС по защите от НСД.	ПК-5; ПК-10; ПК-15

Варианты тестового задания

001. Поставьте в соответствие термин и его определение:

доступ к информации<->возможность получения информации и её использования;

конфиденциальность информации<->обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя;

предоставление информации<->действия, направленные на получение информации определённым кругом лиц или передачу информации определённому кругу лиц;

распространение информации<->действия, направленные на получение информации неопределённым кругом лиц или передачу информации неопределённому кругу лиц;

002. Согласно 149-ФЗ от 27.07.2006 информация это:

а) сведения (сообщения, данные) независимо от формы их представления

б) сведения независимо от формы их представления

в) знания о предметах, фактах, идеях и т. д., которыми могут обмениваться люди в рамках конкретного контекста

г) знания относительно фактов, событий, вещей, идей и понятий, которые в определённом контексте имеют конкретный смысл

д) сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации

003. Информация в зависимости от категории доступа от порядка её предоставления или распространения подразделяется на:

а) общедоступную информацию

б) на информацию ограниченного доступа

в) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

г) информацию, свободно распространяемую

д) информацию, которая подлежит предоставлению или распространению;

е) информацию, распространение которой в Российской Федерации ограничивается или запрещается

004. Сведения о лицах, осуществляющих негласное содействие правоохранительным органам, составляют:

а) государственную тайну

б) тайну следствия

в) банковскую тайну

г) адвокатскую тайну

д) персональные данные

005. Аттестация объектов информатизации – это:

а) комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что

объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утверждённых Гостехкомиссией России

б) форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, документам по стандартизации, принятым Гостехкомиссией (ФСТЭК) России, или условиям договоров с выдачей или продлением «Аттестата соответствия»

в) документальное удостоверение соответствия продукции или иных объектов, процессов обработки информации или оказания информационных услуг требованиям технических регламентов, документам по стандартизации, принятых Гостехкомиссией (ФСТЭК) России или условиям договоров с выдачей «Аттестата соответствия»

006. Технические средства и системы, их коммуникации, не предназначенные для обработки информации, но устанавливаемые вместе со средствами обработки информации на объекте информатизации – это:

а) средства обеспечения объекта информатизации

б) система обработки информации

в) автоматизированная система управления

007. Информация в зависимости от категории доступа к ней подразделяется на:

а) общедоступную информацию

б) на информацию ограниченного доступа

в) информацию, свободно распространяемую

г) информацию, которая подлежит предоставлению или распространению;

д) информацию, распространение которой в Российской Федерации ограничивается или запрещается

008. Поставить в соответствие термины и их определения:

Спецпроверка<->проверка объекта информатизации (технического средства) в целях выявления и изъятия возможно внедрённых закладочных устройств.

Специсследование<->исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации.

Спецобследование<->комплекс инженерно-технических мероприятий, проводимых с использованием специализированных технических средств, с целью выявления возможно внедрённых электронных средств съёма информации в ограждающих конструкциях, мебели и предметах интерьера защищаемого помещения.

009. Цель аттестации объекта информатизации:

а) оценка соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации

б) проведение комплекса мер по приведению объекта информатизации к требуемому уровню безопасности информации

в) проведение комплекса мер по приведению объекта информатизации к требуемому уровню безопасности информации с выдачей «Аттестата соответствия»

г) оценка соответствия применяемого комплекса мер и средств защиты требуемому уровню информационной безопасности

010. К объектам информатизации, аттестуемым по требованиям безопасности информации, относятся:

а) автоматизированные системы различного уровня и назначения

б) системы связи, отображения и размножения, предназначенные для обработки и передачи информации, подлежащей защите, вместе с помещениями, в которых они установлены

в) помещения, предназначенные для ведения конфиденциальных переговоров

г) кабельные и радиолинии связи, предназначенные для передачи информации, подлежащей защите

д) средства вычислительной техники, предназначенные для обработки информации ограниченного распространения, вновь вводимые в эксплуатацию

е) средства вычислительной техники, предназначенные для обработки информации, распространение которой в РФ запрещено или ограничено

011. Органы по аттестации объектов информатизации аккредитуются:

а) ФСТЭК России

б) ФСБ России

в) ФСТЭК России и ФСБ России, в части их касающейся

г) Минюстом России

012. Сведения о лицах, взявших ребёнка из детского дома, составляют:

а) прочие виды профессиональной тайны (врачебная, налоговая, судопроизводства, врачебная, следствия, усыновления и т.д.)

б) государственную тайну

в) банковскую тайну

г) персональные данные

013. Расположите этапы проведения аттестации объектов информатизации в правильном порядке:

Этап 1<->Подача заявки на аттестацию

Этап 2<->Рассмотрение заявки на аттестацию

Этап 3<->Предварительное ознакомление с аттестуемым объектом

Этап 4<->Испытание несертифицированных средств и систем защиты объекта

Этап 5<->Разработка программы и методики аттестационных испытаний

Этап 6<->Заключение договоров на аттестацию

Этап 7<->Проведение аттестационных испытаний объекта информатизации

Этап 8<->Оформление, регистрация и выдача Аттестата соответствия на объект информатизации, отвечающий требованиям по безопасности информации

Этап 9<->Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации

Этап 10<->Рассмотрение апелляций

014. Аттестат соответствия выдаётся владельцу аттестованного объекта информатизации на срок:

а) на период, в течение которого обеспечивается неизменность функционирования объекта информатизации и технологии обработки защищаемой информации, но не более чем на три года

б) на период, в течение которого обеспечивается неизменность функционирования объекта информатизации и технологии обработки защищаемой информации, но не более чем на пять лет

в) не более чем на три года

г) не более чем на пять лет

015. Аттестация объектов может носить:

а) добровольный характер

б) обязательный характер
в) принудительный характер
г) смешанный характер

016. Выберите случаи, когда имеет место быть обязательная аттестация объектов информатизации:

а) обработки информации, составляющей государственную тайну
б) управления экологически опасными объектами
в) ведения секретных переговоров
г) управления крупными бизнес-объектами
д) управления воздушным движением

017. Выберите случаи, когда имеет место быть добровольная аттестация объектов информатизации:

а) при организации защиты информации, содержащейся в государственных информационных ресурсах
б) при обработке информации в государственных и муниципальных информационных системах
в) при проведении лицензирующей деятельности по ТЗКИ и СКЗИ
г) при управлении воздушным и железнодорожным движением
д) при обработке информации в ПАО «Газпром» и ПАО «Сбербанк»

018. Выберите пункты, которые должен содержать «Аттестат соответствия»:

а) регистрационный номер;
б) номер и дата утверждения заключения по результатам аттестационных испытаний
в) наименование, адрес и местоположение объекта информатизации
г) класс защищённости автоматизированной системы
д) организационную структуру объекта информатизации и вывод об уровне подготовки специалистов по защите информации
е) список лиц, допущенных к работе на объекте информатизации
ж) план охраны объекта информатизации и мероприятия по экстренному уничтожению информации (в случае необходимости)

019. Выберите пункты, которые должен содержать «Аттестат соответствия»:

а) номера и даты утверждения программы и методики, в соответствии с которыми проводились аттестационные испытания
б) срок действия
в) дату выдачи
г) гриф секретности (конфиденциальности) информации, обрабатываемой на объекте информатизации
д) состав комплекса технических средств обработки информации ограниченного доступа, перечень вспомогательных технических средств и систем, перечень технических средств защиты информации, а также схемы их размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств
е) список лиц, на которых возлагается обеспечение требований по защите информации и контроль за эффективностью реализованных мер и средств защиты информации
ж) список лиц, допущенных к работе на объекте информатизации
з) план охраны объекта информатизации и мероприятия по экстренному уничтожению информации (в случае необходимости)

020. Орган по аттестации рассматривает заявку на аттестацию:

а) в месячный срок

б) в двухнедельный срок

в) в десятидневный срок

г) в двухмесячный срок

021. В схему аттестации включаются работы по предварительному специальному обследованию аттестуемого объекта, проводимые до этапа аттестационных испытаний:

а) в случае недостаточности исходных данных по аттестуемому объекту информатизации

б) по письменному заявлению владельца объекта информатизации (заявителя)

в) во всех случаях

г) по усмотрению органа по аттестации или аттестационной комиссии

022. Расположите в правильном порядке последовательность проведения аттестационных испытаний:

анализ и оценка исходных данных и документации по защите информации на объекте информатизации, оценка правильности категорирования выделенных помещений и объектов информатизации

оценка уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации

специальное обследование объекта информатизации

проведение испытаний отдельных средств и систем защиты информации в испытательных центрах по сертификации продукции по требованиям безопасности информации (при необходимости)

специальные проверки технических средств на наличие возможно внедрённых специальных электронных устройств перехвата информации

специальные проверки помещений на наличие возможно внедрённых специальных электронных устройств перехвата информации

проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте с помощью специальной контрольно-измерительной аппаратуры

анализ результатов специального обследования и аттестационных испытаний, разработка рекомендаций по совершенствованию принятых мер по защите информации от утечки по техническим каналам, закрытию выявленных каналов утечки информации

подготовка отчётной документации – протоколов испытаний и заключения по результатам аттестационных испытаний с выводами комиссии о соответствии (или несоответствии) объекта информатизации установленным требованиям, которая представляется в орган по аттестации для принятия решения о выдаче «Аттестата соответствия»

023. Выберите пункты, которые включает в себя государственный контроль и надзор за соблюдением порядка аттестации объектов информатизации включает в себя:

а) проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации

б) проверку правильности подготовки органами по аттестации отчётных документов и протоколов испытаний

в) своевременное внесение изменений в нормативные и методические документы по безопасности информации

г) инспекционный контроль за эксплуатацией аттестованных объектов информатизации

д) инспекционный контроль за допуском лиц к эксплуатации объектов информатизации

е) проверку правильности подготовки заявителем исходных данных при подготовке к аттестации

024. Контролируемая зона – это:

а) пространство вокруг объекта информатизации, в котором исключено неконтролируемое пребывание посторонних лиц, а также движение транспортных средств

б) пространство вокруг объекта информатизации, в котором исключено пребывание посторонних лиц, а также движение транспортных средств

в) пространство вокруг объекта информатизации, в котором исключено пребывание посторонних лиц и неконтролируемой пребывание пользователей системы, а также движение транспортных средств

025. Защищаемое помещение – это

а) специально выделенное помещение, в котором планируется в ходе закрытых переговоров, совещаний, встреч обсуждать информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну

б) специально выделенное помещение, в котором планируется в ходе закрытых переговоров, совещаний, встреч обсуждать информацию, содержащую сведения, составляющие государственную тайну

в) специально выделенное помещение, в котором планируется в ходе закрытых переговоров, совещаний, встреч обсуждать любую информацию ограниченного распространения

026. Выберите, к каким классам защиты относятся автоматизированные системы с многопользовательским режимом обработки информации:

а) 1В
б) 1Г
в) 2А
г) 3А
д) 3Б

027. Выберите, к каким классам защиты относятся автоматизированные системы с многопользовательским режимом обработки информации:

а) 1Д
б) 1В
в) 1Г
г) 2А
д) 3А
е) 3Б

028. Третья группа защищённости автоматизированной системы включает АС:

а) в которых работает один пользователь, допущенный ко всей информации АС, размещённой на носителях одного уровня конфиденциальности. Группа содержит классы – 3Б и 3А

б) в которых работает один пользователь, допущенный ко всей информации АС, размещённой на носителях одного уровня конфиденциальности. Группа содержит классы – 3В, 3Б и 3А

в) в которых работает несколько пользователей, имеющие одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит классы – 3Б и 3А

г) в которых работает несколько пользователей, имеющие одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит классы – 3В, 3Б и 3А

029. Вторая группа защищённости автоматизированной системы включает АС:

а) в которых работает несколько пользователей, имеющие одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А

б) в которых работает один пользователь, допущенный ко всей информации АС, размещённой на носителях одного уровня конфиденциальности. Группа содержит классы – 2Б и 2А

в) в которых работает несколько пользователей, имеющие разные права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит классы – 2Б и 2А

г) в которых работает несколько пользователей, имеющие разные права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит классы – 2В, 2Б и 2А

030. Первая группа защищённости автоматизированной системы включает АС:

а) в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности, в которых работает несколько пользователей, и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А

б) в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности, в которых работает несколько пользователей, и не все пользователи имеют право доступа ко всей информации АС. Группа содержит четыре классов – 1Г, 1В, 1Б и 1А

в) в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности, в которых работает несколько пользователей, и все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А

г) в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности, в которых работает только один пользователь, имеющий право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А

031. Для защищённости АС от НСД установлено:

а) 9 классов

б) 8 классов

в) 6 классов

г) 5 классов

032. Выберите, в автоматизированных системах каких классов защиты пользователи имеют равные полномочия на доступ к конфиденциальной информации:

а) 1Д

б) 1В

в) 1Г

г) 2А

д) 2Б

е) 2В
ж) 3А
з) 3Б

033. Выберите, в автоматизированных системах каких классов защиты пользователи имеют разные полномочия на доступ к конфиденциальной информации:

а) 1Д
б) 1В
в) 1Г
г) 2А
д) 2Б
е) 2В
ж) 3А
з) 3Б

034. Состав и содержание, а также форма программ и методик аттестационных испытаний определены в:

а) ГОСТ РО 0043-004-2013
б) ГОСТ РО 0043-002-2012
в) ГОСТ РО 0043-001-2012
г) ГОСТ РО 0044-001-2013

035. Канал утечки информации – это:

а) совокупность источника информации, приёмника информации, а также физической среды, по которой происходит распространение информации от источника к приёмнику

б) совокупность источника информации, приёмника информации, а также физической среды, по которой происходит распространение информации от источника к приёмнику и обратно в симплексном режиме

в) совокупность источника информации, приёмника информации, а также физической среды, по которой происходит распространение информации от источника к приёмнику и обратно в полнодуплексном режиме

г) совокупность источника информации, приёмника информации, а также физической среды, по которой происходит распространение информации от источника к приёмнику и обратно в дуплексном режиме

036. Выберите технические средства, которые могут относиться к ОТСС:

а) средства вычислительной техники
б) средства и системы передачи данных
в) информационные системы
г) средства тиражирования документов
д) технические средства приёма и передачи информации
е) системы звукозаписи и звукоусиления
ж) средства и системы охранной и пожарной сигнализации
з) системы кондиционирования
и) оконечные устройства телефонной связи
к) системы радиовещания;
л) телевизоры
м) чайники

037. Выберите технические средства, которые могут относиться к ВТСС:

а) средства вычислительной техники

б) средства и системы передачи данных
в) информационные системы
г) средства тиражирования документов
д) технические средства приёма и передачи информации
е) системы звукозаписи и звукоусиления
ж) средства и системы охранной и пожарной сигнализации
з) системы кондиционирования
и) оконечные устройства телефонной связи
к) системы радиовещания;
л) телевизоры
м) чайники

038. Выберите методы проверок и испытаний, применяемые при проведении аттестационных испытаний:

а) Экспертно-документальный метод
б) Инструментальные (инструментально-расчётные) измерения и оценка защищённости
в) Оценка функционирования средств защиты информации от несанкционированного доступа
г) Расчётно-аналитические методы с применением 3D-моделирования
д) Методы стохастического наблюдения и измерения электромагнитных полей вокруг защищаемого объекта

039. Выберите основные группы механизмов защиты АС от НСД:

а) механизмы управления доступом
б) механизмы регистрации и учёта
в) механизмы криптографической защиты
г) механизмы контроля целостности
д) механизмы контроля действий пользователей
е) механизмы распределения ключей защиты
ж) механизмы защиты субъектов доступа

040. Аттестационные комиссии формируются:

а) из числа как штатных сотрудников органа по аттестации
б) из числа специалистов в различных направлениях защиты информации других предприятий и организаций
в) из числа штатных сотрудников органа по аттестации и специалистов в различных направлениях защиты информации других предприятий и организаций

Критерии оценки теста:

Оценка	Количество правильных ответов, %	Количество правильных ответов
«неудовлетворительно»	0…49%	0…19
«удовлетворительно»	50…67%	20…27
«хорошо»	68…82%	28…33
«отлично»	83…100%	34…40

Тест считается сданным, если студент получает оценку «удовлетворительно» и выше

Контрольные вопросы для зачёта

1. Организационная структура системы аттестации ОИ и их функции. Какие ОИ подлежат обязательной аттестации.
2. Федеральные органы по аттестации и их функции.

3. Органы по аттестации объектов и их функции. Задачи и функции органа по аттестации.
4. Деятельность аттестационных комиссий
5. Права, обязанности и ответственность органов по проведению аттестации.
6. Аккредитация испытательных лабораторий и органов по сертификации средств защиты информации по требованию безопасности информации. Порядок аккредитации.
7. Контроль и надзор за деятельностью аккредитованных испытательных лабораторий и органов по сертификации.
8. Заявители и их функции. Заявка на проведение аттестации ОИ.
9. Порядок проведения аттестации объектов информатизации. Содержание заявок.
10. Порядок взаимодействия заявителя и органа по проведению аттестации.
11. Испытательные центры сертификации продукции по требованию безопасности. ИХ функции.
12. Исходные данные и документация, представляемая заявителем для проведения аттестации.
13. Составляющие аттестационных испытаний объектов информатизации. Программа аттестации на объектах.
14. Проведение аттестации объектов информатизации. Этапы аттестации.
15. Порядок проведения аттестационных испытаний АС. Основные составляющие.
16. Порядок проведения аттестационных испытаний ВП. Основные составляющие.
17. Заключительный этап аттестации ОИ. Условия получения аттестата соответствия.
18. Что должно содержать заключение аттестационной комиссии.
19. Оформление, регистрация и выдача «Аттестата соответствия».
20. Эксплуатация аттестованного объекта.
21. Рассмотрение апелляций по вопросам аттестации.
22. Аттестационные испытания АС. Что входит в изучение технологического процесса обработки, передачи и хранения информации.
23. Аттестационные испытания АС. Что входит в изучение соответствия организационно-техническим требованиям по ЗИ.
24. Аттестационные испытания АС. Что входит в проверку требований по ЗИ от утечки по цепям заземления и питания.
25. Аттестационные испытания АС. Что входит в испытания на соответствие требованиям по ЗИ от НСД.
26. Аттестационные испытания ВП. Что входит в проверку требований по ЗИ от утечки за счёт ПЭМИН.
27. Аттестационные испытания ВП. Что входит в проверку систем ЗИ.
28. Аттестационные испытания ВП. Что входит в проверку систем ВТСС на отсутствие акустоэлектрических преобразований.
29. Спецобследование ЗП по поиску работающих радиозакладок. Использование индикаторов поля.
30. Спецобследование ЗП по поиску временно отключённых закладных устройств. НРЛ.

Критерии оценки зачёта

Билеты для зачёта включают два вопроса. Ответ на зачёте оценивается до 40 баллов.

Ответ на вопрос № 1 – оценивается до 20 баллов

Ответ на вопрос № 2 – оценивается до 20 баллов

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

основные

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

2. Закон РФ от 21.07.1993 N 5485-1 (ред. от 29.07.2018) «О государственной тайне» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_2481/ /, свободный. – Загл. с экрана.

3. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну». [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77

4. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс] : Режим доступа : https://base.garant.ru/5921891/, свободный в комм. версии. – Загл. с экрана.

5. Рекомендации стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. [Электронный ресурс] : Режим доступа : https://base.garant.ru/71066790/, свободный в комм. версии. – Загл. с экрана.

6. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77, свободный в комм. версии. – Загл. с экрана.

дополнительные

7. Руководящий документ «Защита информации. Специальные защитные знаки. Классификация и общие требования», утверждённым решением председателя Гостехкомиссии от 25.07.1997 г., (По состоянию на 18 февраля 2018 г.) [Электронный ресурс] : Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-25-iyulya-1997-g-2 свободный. – Загл. с экрана.

Литература

1. Тумбинская, М. В. Защита информации на предприятии : учебное пособие для вузов / М. В. Тумбинская, М. В. Петровский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 184 с. — ISBN 978-5-507-52967-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/463043. — Режим доступа: для авториз. пользователей.

2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 5-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2026. — 384 с. — (Высшее образование). — DOI: https://doi.org/10.29039/02005-0. - ISBN 978-5-369-02005-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2233509. – Режим доступа: по подписке.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Онлайн-курс «Аттестация объектов информатизации по требованиям безопасности информации» Автор: Ольга Сапронова. [Электронный ресурс] : Режим доступа : https://www.intuit.ru/studies/courses/3648/890/info свободный. – Загл. с экрана.

Национальная электронная библиотека (НЭБ) www.rusneb.ru

ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:
1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

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

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 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, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.

Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика практических занятий соответствует программе дисциплины.

Практическое занятие 1 (10 ч.)

Задание.

1. Разработать заявку для проведения аттестации объекта информатизации предложенной организации по следующей форме

Кому:_____

(наименование органа по аттестации и его адрес)

З А Я В К А
на проведение аттестации объекта информатизации

1. *(наименование заявителя)* просит провести аттестацию *(наименование объекта информатизации)* на соответствие требованиям по безопасности информации:_____

2. Необходимые исходные данные по аттестуемому объекту информатизации прилагаются.

3. Заявитель готов предоставить необходимые документы и условия для проведения аттестации.

4. Заявитель согласен на договорной основе оплатить расходы по всем видам работ и услуг по аттестации указанного в данной заявке объекта информатизации.

5. Дополнительные условия или сведения для договора:

5.1. Предварительное ознакомление с аттестуемым объектом предлагаю провести в период _____

5.2. Аттестационные испытания объекта информатики предлагаю провести в период _____

5.3. Испытания несертифицированных средств и систем информатизации *(наименование средств и систем)* предусмотрено провести в испытательных центрах (лабораториях) *(наименование испытательных центров)* в период _____ (или предлагается провести непосредственно на аттестуемом объекте в период _____)

Другие условия (предложения).

печать

Руководитель (органа заявителя)

(подпись, дата) (Фамилия, И.О.)

Приложение к форме "Заявки..."

Исходные данные по аттестуемому объекту информатизации готовятся на основе следующего перечня вопросов

1. Полное и точное наименование объекта информатизации и его назначение.

2. Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень секретности (конфиденциальности) обрабатываемой информации определен (в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия).

3. Организационная структура объекта информатизации.

4. Перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация (расположенных в помещениях, где она циркулирует).

5. Особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны.

6. Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.

7. Общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации.

8. Наличие и характер взаимодействия с другими объектами информатизации.

9. Состав и структура системы защиты информации на аттестуемом объекте информатизации.

10. Перечень технических и программных средств в защищённом исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.

11. Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков (по отношению к предприятию, на котором расположен аттестуемый объект информатизации) лицензий на проведение подобных работ.

12. Наличие на объекте информатизации (на предприятии, на котором расположен объект информатизации) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных).

13. Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).

14. Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

Указания по выполнению заданий:
1. Преподаватель выдаёт каждому студенту структуру и штат организации.
2. Студенты должны определить территориальный орган ФСТЭК России и орган по аттестации, ближайший к организации, аккредитованной во ФСТЭК России.

Материально-техническое обеспечение занятия:
компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлены:
– лицензионное ПО MS Windows 7 и новее;
– лицензионное ПО MS Office 2010 и новее.

Практическое задание № 2, 3 (18 ч.) – Разработка программы и методики аттестационных испытаний

Задания:
1. Разработать программу и методики аттестационных испытаний объекта информатизации.

Указания по выполнению заданий:
1. По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом органом по аттестации разрабатываются программа аттестационных испытаний, предусматривающая перечень работ и их продолжительность, методики испытаний (или используются типовые методики), определяются количественный и профессиональный состав аттестационной комиссии, назначаемой органом по аттестации объектов информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации или привлечения испытательных центров (лабораторий) по сертификации средств защиты информации по требованиям безопасности информации.
2. Порядок, содержание, условия и методы испытаний для оценки характеристик и показателей, проверяемых при аттестации, соответствия их установленным требованиям, а также применяемые в этих целях контрольная аппаратура и тестовые средства определяются в методиках испытаний различных видов объектов информатизации.
3. Программа аттестационных испытаний согласовывается с «заявителем».

Материально-техническое обеспечение занятия:
компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлены:
– лицензионное ПО MS Windows 7 и старше;
– лицензионное ПО MS Office 2010 и старше.

По результатам практических занятий обучающиеся составляют отчёты. Отчёт составляется в электронной форме с использованием ПКП MS Office 2007 и выше и передаётся преподавателю посредством оговорённой формы связи.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины: 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, утверждённых 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.

В результате освоения дисциплины обучающийся должен:

Знать: нормативные правовые акты, методические документы, национальные стандарты в области аттестации объектов информатизации на соответствие требованиям по защите информации;

Уметь: разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите 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 составления необходимых документов при проведении аттестации объектов информатизации