МИНОБРНАУКИ РОССИИ

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

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

ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

По направлению подготовки 10.03.01 «Информационная безопасность»
профиль «Организация и технология защиты информации»
Уровень квалификации выпускника (*бакалавр*)

Форма обучения (*очная*)

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Организационное обеспечение аттестации объектов информатизации
Рабочая программа дисциплины

Составитель:
д.т.н, профессор В.В. Арутюнов

Ответственный редактор
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 10 от 20.05.2021

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины (модуля)

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

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

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

Компетенция (код и название)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК-2.3.1 Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации	Знать: национальные, межгосударственные и международные стандарты в области защиты информации; Уметь: использовать нормативно-технические документы и стандарты по обеспечению безопасности объекта защиты; Владеть: навыками использования стандартов в области защиты информации, руководящих и методических документов уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации
	ОПК-2.3.2 Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от	Знать: процедуры контроля функционирования системы защиты информации; Уметь: документировать процедуры и результаты контроля функционирования системы защиты информации; Владеть: навыками проведения испытания программно-технических средств защиты

	НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям	информации;
	ОПК-2.3.3 Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям	Знать: порядок разработки программ и методик испытаний опытного образца программно-технического средства защиты информации; Уметь: разрабатывать программы и методики испытаний опытного образца программно-технического средства защиты информации; Владеть: навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации;
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 защиты информации ограниченного доступа; Уметь: пользоваться нормативными правовыми актами, методическими документами, национальными стандартами в области защиты информации ограниченного доступа; Владеть: навыками аттестации объектов информатизации на соответствие требованиям по защите информации;
	ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на	Знать: правила формирования заключения по результатам аттестации выделенных (защищаемых) помещений; Уметь: разрабатывать программы и методики аттестационных испытаний выделенных

	соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации	(защищаемых) помещений на соответствие требованиям по защите информации; Владеть: навыками проведения аттестационных испытаний выделенных (защищаемых) помещений;
	ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации	Знать: порядок подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации; Уметь: пользоваться нормативными актами для получения аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации; Владеть: навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации;
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 и международные стандарты в области защиты информации; Уметь: пользоваться нормативными правовыми актами, методическими документами, национальными стандартами в области защиты информации; Владеть: навыками использования стандартов в области защиты информации;
	ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях	Знать: назначение, функции, условия функционирования объектов и систем обработки информации ограниченного

	функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации	доступа; Уметь: анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа; Владеть: методами анализа функционирования систем обработки информации ограниченного доступа, установленных на объектах информатизации;
	ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	Знать: порядок создания системы защиты информации в организации; Уметь: аналитически обосновывать необходимость создания системы защиты информации в организации; Владеть: навыком разработки аналитического обоснования необходимости создания системы защиты информации;
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 действующими нормативными и методическими документами	Знать: технологический процесс защиты информации и процедуру разработки технических заданий и планов в соответствии с действующими нормативными и методическими документами; Уметь: пользоваться действующими нормативными и методическими документами в области защиты информации; Владеть: навыками организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами;
	ПК-15.2 Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации;	Знать: действующие национальные, межгосударственные и международные стандарты в области защиты информации; Уметь: применять национальные, межгосударственные и

	применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке	международные стандарты в области защиты информации; Владеть: навыками освоения нормативных и методических документов по информационной безопасности на английском языке
	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	Знать: порядок выполнения работ, а также действующее законодательство Российской Федерации при решении вопросов, касающихся защиты информации; Уметь: пользоваться национальными законодательными документами при решении вопросов, касающихся защиты информации; Владеть: навыками по контролю над соблюдением установленного порядка выполнения работ по защите информации.

1.3. Место дисциплины в структуре основной образовательной программы

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

Для освоения дисциплины (модуля) необходимы компетенции, сформированные в ходе изучения следующих дисциплины и прохождения практики: Защита информации от несанкционированного доступа, Экономика защиты информации.

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

2. Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 76 ч., в том числе контактная работа обучающихся с преподавателем 40 ч., самостоятельная работа обучающихся - 36 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Назначение и общая характеристика аттестации и сертификации в области защиты информации	7	2		4			8	опрос
2	Основные требования к защищённости базовых объектов информатизации	7	2		4			8	опрос
3	Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации	7	6		4			10	опрос
4	Порядок проведения аттестации объектов информатизации	7	6		12			10	опрос, контрольная работа
	Итого		**16**		**24**			**36**	

3. Содержание дисциплины (модуля)

№	Наименование раздела дисциплины	Содержание
1	**Тема 1. Назначение и общая характеристика аттестации и сертификации в области защиты информации**	Предмет и содержание дисциплины, методы изучения, основная литература, контроль освоения дисциплины. Основные цели механизмов лицензирования и сертификации в России. Базовый нормативный документ в области сертификации и аттестации в России. Цели и принципы сертификации. Понятие декларации о соответствии и обязательной

		сертификации. Содержание декларации о соответствии. Сущность и состав сертификата соответствия. Основные схемы декларирования соответствия продукции. Основные принципы проведении сертификационных испытаний средств защиты информации. Сертификация продукции на международном уровне.
2	**Тема 2. Основные требования к защищённости базовых объектов информатизации**	Основная цель аттестации объектов информатизации. Базовые нормативные правовые акты в сфере сертификации и аттестации. Основные схемы аттестации объектов информатизации. Аттестация автоматизированных систем и средств вычислительной техники (СВТ) в России в соответствии с руководящими документами (РД) ФСТЭК России. Перечень требований к защищенности автоматизированных систем в зависимости от класса защищенности. Перечень требований к защищенности СВТ в зависимости от класса защищенности. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей. Классификация межсетевых экранов по уровню защищённости от НСД.
3	**Тема 3. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации**	Основные элементы системы аттестации объектов информатизации по требованиям безопасности информации. Структура органов по аттестации объектов информатизации, которые аккредитуются ФСТЭК России. Основные функции федерального органа по сертификации и аттестации. Базовые функции

		органов по аттестации объектов информатизации. Основные работы испытательных центров (лабораторий) по сертификации продукции. Базовые виды работ заявителей аттестуемых объектов информатизации.
4	**Тема 4. Порядок проведения аттестации объектов информатизации**	Основные этапы проведения аттестации объектов информатизации. Содержание, порядок государственного контроля и надзора по аттестации объектов информатизации. Содержание заявки заявителя для получения «Аттестата соответствия». Порядок проведения аттестационных испытаний. Исходные данные и документация, представляемая заявителем органу по аттестации. Основные работы при проведении специального обследования аттестуемого объекта. Базовые работы, проводимые при аттестации объектов информатизации для каждого технического средства обработки информации (ТСОИ). Основные работы при аттестации выделенного помещения. Структура заключения аттестационной проверки объекта информатизации. Содержание протокола аттестационных испытаний. Структура «Аттестата соответствия» объекта информатизации (выделенного помещения) требованиям по безопасности информации. Сущность контроля состояния защиты информации с целью своевременного выявления и предотвращения утечки информации по

		техническим каналам на предприятии. Категорирование объектов и определение режимных зон внутри них.

4. Образовательные технологии

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

№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1.	Назначение и общая характеристика аттестации и сертификации в области защиты информации	Лекция 1 Практическое занятие 1	Вводная лекция с использованием видеоматериалов опрос
2.	Основные требования к защищённости базовых объектов информатизации	Лекция 2 Практическое занятие 2	Лекция с использованием видеопроектора опрос
3.	Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации	Лекция 3 Практическое занятие 3	Лекция с использованием видеопроектора опрос
4.	Порядок проведения аттестации объектов информатизации	Лекция 4 Практическое занятие 4 Контрольная работа	Лекция с использованием видеопроектора Опрос Подготовка к контрольной с использованием материалов лекций и литературы

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* *- контрольная работа (темы 3-4)*	 *10 баллов* *20 баллов*	 *40 баллов* *20 баллов*
Промежуточная аттестация *(традиционная форма)*		*40 баллов*
Итого за семестр *зачёт*		*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	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		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	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	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	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.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		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 *(модулю)*

Примерная тематика опросного задания

1. Базовые органы - регуляторы правовых документов в сфере ИБ в России на федеральном уровне - ПК-10.

2. Объекты информатизации, аттестуемые по требованиям безопасности информации - ПК-5.

3. Основные виды работ, проводимые в соответствии со схемой аттестации - ОПК-2.3.

4. Базовые категории аттестуемых объектов информатизации - ПК-5.

5. Функции органов по аттестации объектов информатизации - ПК-15.

6. Основные группы показателей защищённости СВТ - ПК-15.

Примерная тематика контрольной работы

1. Содержание декларации о соответствии - ПК-10.
2. Особенности различных схем декларирования соответствия продукции - ПК-10.
3. Содержание сертификата соответствия - ПК-10.
4. Сведения, содержащиеся в сертификате на продукцию - ОПК-2.3.
5. Базовые уровни сертификации для систем конфиденциального электронного документооборота - ОПК-2.3.
6. Основные виды документов, используемые при проведении сертификационных испытаний - ОПК-2.3.

7. Базовые разделы методики сертификационных испытаний - ОПК-2.3.
8. Содержание протокола сертификационных испытаний - ПК-10.
9. Основные группы классификация автоматизированных систем в соответствии с требованиями по защите информации - ПК-15.
10. Базовые группы показателей защищённости СВТ - ПК-15.
11. Основные группы требований к защищенности АС в зависимости от класса их защищенности - ПК-15.
12. Классификация МЭ по уровню контроля отсутствия незадекларированных возможностей - ПК-15.
13. Функции органов по аттестации объектов информатизации - ПК-5.
14. Состав программы аттестационных испытаний - ПК-5.
15. Базовые действия при аттестации выделенного помещения - ПК-5.
16. Основные разделы протокола аттестационных испытаний - ПК-5.

Промежуточная аттестация (примерные вопросы к зачету)

1. Основные цели сертификации в России в области защиты информации - ОПК-2.3.
2. Характеристика базовых органов - генераторов правовых документов в сфере ИБ в России на федеральном уровне - ПК-15.
3. Основные принципы, обеспечивающие эффективность сертификации - ОПК-2.3.
4. Содержание декларации о соответствии - ОПК-2.3.
5. Особенности различных схем декларирования соответствия продукции - ОПК-2.3.
6. Основные принципы проведении сертификационных испытаний средств защиты информации - ОПК-2.3.
7. Основные разделы пользовательской документации для импортного ПО - ПК-15.
8. Базовые объекты информатизации, аттестуемые в соответствии с требованиям безопасности информации - ПК-5.
9. Основные виды работ, проводимые в соответствии со схемой аттестации - ПК-10.
10. Перечень необходимых работ для выбора схемы аттестации - ПК-10.
11. Классификация автоматизированных систем в соответствии с требованиями по защите информации - ПК-15.

12. Классификация СВТ в соответствии с требованиями по защите информации - ПК-15.
13. Основные требования по защите, предъявляемые к межсетевым экранам - ПК-15.
14. Классификация программного обеспечения по уровню контроля отсутствия недекларированных возможностей - ПК-15.
15. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации - ПК-10.
16. Основные работы заявителей для проведения аттестации объектов информатизации - ПК-5.
17. Базовые этапы проведения аттестации - ПК-5.
18. Содержание программы аттестационных испытаний - ПК-5.
19. Основные категории аттестуемых объектов информатизации - ПК-5.
20. Базовые зоны безопасности аттестуемых объектов информатизации - ПК-5.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

а) основная литература

1. Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации - Режим доступа: URL: https://www.intuit.ru/studies/courses/3648/890/info

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

б) дополнительная литература

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

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

3. Кривенцев В.А., Селифанов В.В., Звягинцева П.А. Проведение аттестационных

испытаний автоматизированной системы в защищенном исполнении // Интерэкспо Гео-Сибирь. 2019. Т. 9. С. 30-34. - Режим доступа: URL: . 2019. Т. 9. С. 30-34.

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

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

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

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

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

Перечень БД и ИСС

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

7. Материально-техническое обеспечение дисциплины/модуля

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

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

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

Состав программного обеспечения (ПО)

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

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

Тема 1 (4 ч.). Характеристика сертификации в области защиты в России

Вопросы для обсуждения:

1. Базовые цели реализации сертификации в России - ОПК-2.3.
2. Основные уровни сертификации для систем конфиденциального электронного документооборота - ОПК-2.3.
3. Базовые органы - генераторы правовых документов в сфере ИБ в России на федеральном уровне - ПК-10.
4. Основные принципы, соблюдение которых необходимо при проведении сертификационных испытаний средств защиты информации - ПК-5.
5. Понятие декларации о соответствии - ПК-15.

6. Основные документы, необходимые для регистрации системы добровольной сертификации - ПК-15.

7. Структура сертификата соответствия - ПК-5.

8. Содержание декларации о соответствии - ПК-10.

Список литературы:

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

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

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

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

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

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

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

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

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

Тема 2 (4 ч.). Аттестация автоматизированных систем, средств вычислительной техники и межсетевых экранов в России

Вопросы для изучения и обсуждения:

1. Основные схемы проведения аттестации объектов информатизации - ОПК-2.3.
2. Базовые классы защищённости автоматизированных систем - ПК-15.
3. Основные группы защищённости СВТ - ПК-15.
4. Классификация программного обеспечения по уровню контроля отсутствия недекларированных возможностей - ПК-5.

5. Классификация межсетевых экранов по уровню защищённости от НСД - ПК-5.
6. В каких случаях аттестация носит обязательный или добровольный характер? - ПК-10.
7. Нормативные правовые акты, определяющие основные принципы и организационную структуру системы аттестации и порядок проведения аттестации - ОПК-2.3.
8. Основные требования по защите межсетевых экранов - ПК-5.
9. Основные подсистемы автоматизированных систем, для которых устанавливаются требования по их защищённости - ПК-10.

Список литературы:

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

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

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

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

Кривенцев В.А., Селифанов В.В., Звягинцева П.А. Проведение аттестационных испытаний автоматизированной системы в защищенном исполнении // Интерэкспо Гео-Сибирь. 2019. Т. 9. С. 30-34. - Режим доступа: URL: . 2019. Т. 9. С. 30-34.

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

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

Тема 3 (4 ч.). Основные элементы системы аттестации объектов информатизации по требованиям безопасности информации

Вопросы для обсуждения:

1. Структурный состав системы аттестации объектов информатизации по требованиям безопасности информации - ПК-5.
2. Основные элементы органов по аттестации объектов информатизации - ПК-15.

3. Базовые функции федерального органа по сертификации - ПК-15.
4. Основные функции органов по аттестации объектов информатизации - ПК-10.
5. Базовые элементы системы аттестации объектов информатизации по требованиям безопасности информации - ПК-5.
6. Основные работы заявителей для проведения аттестации объектов информатизации - ПК-10.
7. Какую работу проводят испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации? - ОПК-2.3.
8. Основные разделы заявки заявителя на проведение аттестации - ОПК-2.3.

Список литературы:

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

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

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

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

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

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

Тема 4 (4 ч.). Основные этапы проведения аттестации объектов информатизации

Вопросы для обсуждения:

1. Сведения, представляемые заявителем для проведения аттестационных испытаний - ПК-5.
2. Основные работы, проводимые при проведении специального обследования аттестуемого объекта - ПК-15.
3. Базовые работы, проводимые при аттестации выделенного помещения - ПК-10.

4. Содержание программы аттестационных испытаний - ПК-10.
5. Основные категории аттестуемых объектов информатизации - ПК-10.
6. Основные этапы проведения аттестации объектов информатизации - ПК-15.
7. Что реализуется на начальном этапе проведения аттестации объектов информатизации? - ПК-5.
8. Что включает этап проведения аттестационных испытаний объекта информатизации? - ПК-5.
9. Основные разделы заявки заявителя на получение «Аттестата соответствия» - ОПК-2.3.
10. Содержание протокола аттестационных испытаний - ОПК-2.3.

Список литературы:

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

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

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

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

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

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

Приложение 1

АННОТАЦИЯ

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

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

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

Дисциплина (модуль) направлена на формирование следующих компетенций:

ОПК-2.3 - способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;

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

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

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.

В результате освоения дисциплины обучающийся должен:

- знать: национальные, межгосударственные и международные стандарты в области защиты информации; процедуры контроля функционирования системы защиты информации; порядок разработки программ и методик испытаний опытного образца программно-технического средства защиты информации; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа; правила формирования заключения по результатам аттестации выделенных (защищаемых) помещений; порядок подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации; нормативные правовые акты, методические документы, национальные и международные стандарты в области защиты информации; назначение, функции, условия функционирования объектов и систем обработки информации ограниченного доступа; порядок создания системы защиты информации в организации; технологический процесс защиты информации и процедуру разработки технических заданий и планов в

соответствии с действующими нормативными и методическими документами; действующие национальные, межгосударственные и международные стандарты в области защиты информации; порядок выполнения работ, а также действующее законодательство Российской Федерации при решении вопросов, касающихся защиты информации;

- уметь: использовать нормативно-технические документы и стандарты по обеспечению безопасности объекта защиты; документировать процедуры и результаты контроля функционирования системы защиты информации; разрабатывать программы и методики испытаний опытного образца программно-технического средства защиты информации; пользоваться нормативными правовыми актами, методическими документами, национальными стандартами в области защиты информации ограниченного доступа; разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации; пользоваться нормативными актами для получения аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации; пользоваться нормативными правовыми актами, методическими документами, национальными стандартами в области защиты информации; анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа; аналитически обосновывать необходимость создания системы защиты информации в организации;

- владеть: навыками использования стандартов в области защиты информации, руководящих и методических документов уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации; навыками проведения испытания программно-технических средств защиты информации; навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками аттестации объектов информатизации на соответствие требованиям по защите информации; навыками проведения аттестационных испытаний выделенных (защищаемых) помещений; навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации; навыками использования стандартов в области защиты информации; методами анализа функционирования систем обработки информации ограниченного доступа, установленных на объектах информатизации; навыком разработки аналитического обоснования необходимости создания системы защиты информации; навыками организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами; навыками освоения нормативных и методических документов по информационной безопасности на английском языке; навыками по контролю над соблюдением установленного порядка выполнения работ по защите информации.

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

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