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 комплексной защиты информации

АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профили) подготовки:
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Аттестация объектов информатизации
Рабочая программа дисциплины
Составитель:
Кандидат военных наук, доцент кафедры КЗИ Д.Н. Баранников

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№_10_ от__20.05.2021 г._____

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. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с индикаторами достижения компетенций

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 защиты информации ограниченного доступа и 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:* • *навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по за-*

	требованиям по защите информации	*щите информации*
ПК-10 *Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности*	*ПК-10.1* *Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации*	*Знать:* • *процедуру организации установки и настройки технических, программных (программ-но-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации.*
	ПК-10.2 *Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации*	*Владеть:* • *навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации*
	ПК-10.3 *Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации*	*Уметь:* •• *разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации*
ПК-8 Способен осуществлять мониторинг и аудит защищенности информации в автоматизированных системах	*ПК-8.1* *Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации*	*Знать:* • *основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах;* • *организационные меры по защите информации.*
	ПК-8.2 *Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы*	*Уметь:* • *анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей без-опасности информации в автоматизированных системах; вести протоколы и журналы учёта при осуществлении аудита*

	и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем	*систем защиты информации автоматизированных систем*
	ПК-8.3 *Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы*	*Владеть:* • *навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Аттестация объектов информатизации» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Безопасность операционных систем», «Методы и средства защиты информации от утечки по техническим каналам», «Безопасность программного обеспечения автоматизированных систем», «Базы данных, системы управления базами данных», «Физические основы защиты информации».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Информационная безопасность телекоммуникационных систем», «Преддипломная практика», «Аудит информационной безопасности».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _2_ з.е., _76__ ч., в том числе контактная работа обучающихся с преподавателем _40_ ч., промежуточная аттестация __ ч., самостоятельная работа обучающихся _36_ ч.

№ п/п	Темы дисциплины/	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	*Правовые основы аттестации объектов информатизации*	**7**	**2**					**6**	Опрос, выполнение практического задания
2	*Место и роль аттестации объектов информатизации в системе защиты информации.*	**7**	**2**		**4**			**6**	Опрос, выполнение практического задания
3	*Структура системы аттестации объектов информатизации*	**7**	**2**		**4**			**6**	Опрос, выполнение практического задания
4	*Порядок проведения аттестации объекта информатизации*	**7**	**2**		**4**			**6**	Опрос, выполнение практического задания
5	*Порядок проведения аттестационных испытаний защищаемого помещения*	**7**	**4**		**6**			**6**	Опрос, выполнение практического задания
6	*Порядок проведения аттестационных испытаний автоматизированной системы*	**7**	**4**		**6**			**6**	Опрос, выполнение практического задания
	зачет								*зачет по билетам*
	итого:		**16**		**24**			**36**	

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.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
2	*Место и роль аттестации объектов информатизации в системе защиты информации*	*Лекция 2.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
3	*Структура системы аттестации объектов информатизации*	*Лекция 3.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
4	*Порядок проведения аттестации объекта информатизации*	*Лекция 4.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
5	*Порядок проведения аттестационных испытаний защищаемого помещения*	*Лекция 5* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
6	*Порядок проведения аттестационных испытаний автоматизированной системы*	*Лекция 6* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
7	*Анализ источников, каналов распространения и каналов утечки информации*	*Практическое занятие 1*	Выполнение задания
8	*Изучение программно-аппаратных*	*Практическое занятие 2*	Выполнение задания

	средств, реализующих основные функции ЭП		
9	*Изучение принципов работы протоколов аутентификации с использованием доверенной стороны*	*Практическое занятие 3*	Выполнение задания
10	*Проведение анализа информации на предмет целостности*	*Практическое занятие 4*	Выполнение задания
11	*Оценка уязвимости информации*	*Практическое занятие 5*	Выполнение задания
12	*Определение классов защищенности средств вычислительной техники от несанкционированного доступа*	*Практическое занятие 6*	Выполнение задания

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1-3)* *– опрос (темы 4-6)* *– практическое занятие (темы 1-6)*	 *4 балла* *4 балла* *6 баллов*	 *12 баллов* *12 баллов* *36 баллов*
Промежуточная аттестация *экзамен*		*40 баллов*
Итого за дисциплину *экзамен*		*100 баллов*

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

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1.	Темы 1-6	ПК-5; ПК-5.1; ПК-5.2; ПК-5.3; ПК-10; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8; ПК-8.1; ПК-8.2; ПК-8.3	Устный опрос на занятиях
2.	Практические занятия	ПК-5; ПК-5.1; ПК-5.2; ПК-5.3; ПК-10; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8; ПК-8.1; ПК-8.2; ПК-8.3	План практического занятия

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.

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

Перечень устных вопросов для проверки знаний

№	Вопрос	Реализуемая компетенция
1.	Классификация информации в зависимости от порядка её предоставления или распространения	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
2.	Виды информации, доступ к которой должен быть ограничен	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
3.	Нормативные документы по аттестации объектов информатизации	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
4.	Что понимается под объектом информатизации и аттестацией объекта информатизации	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
5.	Определение разведдоступности	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
6.	Определение специальных проверок, специального обследования и специальных исследований	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
7.	Цели аттестации ОИ.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
8.	Виды аттестации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
9.	Общие требования к организации аттеста-	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-

	ции объектов информатизации.	10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
10.	Обязательная аттестация.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
11.	Добровольная аттестация.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
12.	Объекты, подлежащие обязательной аттестации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
13.	Основные составляющие структуры аттестации объектов информатизации	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
14.	Органы по аттестации объектов.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
15.	Требования к органу по аттестации объектов информатизации по требованиям безопасности информации,	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
16.	Лицензирование деятельности предприятий в качестве испытательных центров.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
17.	Требования к деятельности заявителей.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
18.	Этапы проведения аттестации ОИ	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
19.	Испытание несертифицированных средств и систем защиты информации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
20.	Разработка программы и методики аттестационных испытаний.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
21.	Проведение аттестационных испытаний объекта информатизации	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
22.	«Аттестат соответствия»	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
23.	Выявление специальных электронных устройств перехвата информации	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
24.	Технические средства необходимые для проведения аттестации защищаемых помещений	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
25.	Проверка выполнения требований по защите информации от утечки за счёт ПЭМИН.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
26.	Проверка выполнения требований от утечки за счёт наводок на ВТСС.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
27.	Проверка выполнения требований от утечки по цепям электропитания и заземления.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
28.	Классификация АС по защите от НСД.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3

Промежуточная аттестация (примерные вопросы к зачету)

№	Вопрос	Реализуемая компетенция
1.	Организационная структура системы аттестации ОИ и их функции. Какие ОИ подлежат обязательной аттестации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
2.	Федеральные органы по аттестации и их функции	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
3.	Органы по аттестации объектов и их функ-	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-

	ции. Задачи и функции органа по аттестации	10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
4.	Деятельность аттестационных комиссий	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
5.	Права, обязанности и ответственность органов по проведению аттестации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
6.	Аккредитация испытательных лабораторий и органов по сертификации средств защиты информации по требованию безопасности информации. Порядок аккредитации	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
7.	Контроль и надзор за деятельностью аккредитованных испытательных лабораторий и органов по сертификации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
8.	Заявители и их функции. Заявка на проведение аттестации ОИ.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
9.	Порядок проведения аттестации объектов информатизации. Содержание заявок.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
10.	Порядок взаимодействия заявителя и органа по проведению аттестации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
11.	Испытательные центры сертификации продукции по требованию безопасности. ИХ функции.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
12.	Исходные данные и документация, представляемая заявителем для проведения аттестации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
13.	Составляющие аттестационных испытаний объектов информатизации. Программа аттестации на объектах.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
14.	Проведение аттестации объектов информатизации. Этапы аттестации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
15.	Порядок проведения аттестационных испытаний АС. Основные составляющие.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
16.	Порядок проведения аттестационных испытаний ВП. Основные составляющие.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
17.	Заключительный этап аттестации ОИ. Условия получения аттестата соответствия.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
18.	Что должно содержать заключение аттестационной комиссии.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
19.	Оформление, регистрация и выдача «Аттестата соответствия».	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
20.	Эксплуатация аттестованного объекта.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
21.	Рассмотрение апелляций по вопросам аттестации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
22.	Аттестационные испытания АС. Что входит в изучение технологического процесса обработки, передачи и хранения информации.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
23.	Аттестационные испытания АС. Что входит в изучение соответствия организационно-техническим требованиям по ЗИ.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
24.	Аттестационные испытания АС. Что входит в проверку требований по ЗИ от утечки по	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3

	цепям заземления и питания.	
25.	Аттестационные испытания АС. Что входит в испытания на соответствие требованиям по ЗИ от НСД.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
26.	Аттестационные испытания ВП. Что входит в проверку требований по ЗИ от утечки за счёт ПЭМИН.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
27.	Аттестационные испытания ВП. Что входит в проверку систем ЗИ.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
28.	Аттестационные испытания ВП. Что входит в проверку систем ВТСС на отсутствие акустоэлектрических преобразований.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
29.	Спецобследование ЗП по поиску работающих радиозакладок. Использование индикаторов поля.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3
30.	Спецобследование ЗП по поиску временно отключённых закладных устройств. НРЛ.	ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Литература

Основная

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. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. (По состоянию на 8 июля 2018 г.). [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g, свободный. – Загл. с экрана.
4. ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. (По состоянию на 8 июля 2018 г.) [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=261#0193131744513834 64, свободный в комм.версии. – Загл. с экрана.
5. Рекомендации стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. (По состоянию на 8 июля 2018 г.) [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=19063#03281792453677 118, свободный в комм.версии. – Загл. с экрана.

Дополнительная

6. Приказ ФСТЭК России от 17.07.2017 № 133 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и

производству средств защиты конфиденциальной информации» (По состоянию на 8 июля 2018 г.) [Электронный ресурс] : Режим доступа : https://fstec.ru/index?id=1359:prikaz-fstek-rossii-ot-17-iyulya-2017-g-n-133, свободный. – Загл. с экрана.

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/component/attachments/download/316 свободный. – Загл. с экрана.

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

1. 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.10.Сайт

2. Научной электронной библиотеки www.elibrary.ru

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 10 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

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

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

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.

– 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 – проверка сформированности компетенций – ПК-5.1; ПК-5.2; ПК-5.3; ПК-10.1; ПК-10.2; ПК-10.3; ПК-8.1; ПК-8.2; ПК-8.3

Темы учебной дисциплины предусматривают проведение практических работ, 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 работ, выдаваемые преподавателем на каждом занятии.

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

Тематика практических работ соответствует программе дисциплины.

Практическая работа 1 (4 ч.) Порядок проведения аттестационных испытаний автоматизированной системы – ПК-5; ПК-10; ПК-8

Задания:

1. Определение исходных данных для проведения аттестационных испытаний.
2. Создание план-схемы инженерных сетей.

Список литературы:

1. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g.

2. 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

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.

Практическая работа 2 (4 ч.) Изучение программно-аппаратных средств, реализующих основные функции ЭП – ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3

Задания:

1. Определение дестабилизирующего воздействия на защищаемую информацию.
2. Изучение штатных средств защиты информации в операционных системах.
3. Построение одели оценки уязвимости информации.

Список литературы:

1.Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g

2.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

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.

Практическая работа 3 (4 ч.) Изучение принципов работы протоколов аутентификации с использованием доверенной стороны – ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3

Задания:

1. Выполнить запрос на ввод идентификатора со стороны системы защиты.
2. Осуществить ввод пользователем своего идентификатора.

Список литературы:

1. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g.

2. 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

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.

Практическая работа 4 (4 ч.) Создание и администрирование групп пользователей – ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3

Задания:

1. Определить результирующие разрешения пользователей.
2. Назначьте разрешения группам.
3. Необходимо прекратить совместное использования папки.

Список литературы:

1. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994.
2. 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

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.

Практическая работа 5 (6 ч.) Оценка уязвимости информации – ОПК-5.1; ОПК-5.2; ОПК-5.3; ПК-13.1; ПК-13.2; ПК-13.3

Задания:

1. Провести анализ защищенности объекта защиты информации по видам возможных угроз.
2. Определить причины нарушения целостности информации.
3. Определить класс защищенности автоматизированной системы.

Список литературы:

1. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g.
2. 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

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.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Аттестация объектов информатизации» реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата (по направлению подготовки – Безопасность автоматизированных систем) кафедрой Комплексной защиты информации.

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.

Дисциплина направлена на формирование следующих компетенций:

- 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
    - 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
    - ПК-5.3 – Владеет 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 процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации
    - ПК-10.2 – Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации
    - ПК-10.3 – Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации
- ПК-8 – Способен осуществлять мониторинг и аудит защищённости информации в автоматизированных системах
    - ПК-8.1 – Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации
    - ПК-8.2 – Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных

системах; вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем

- ПК-8.3 – Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы

В результате освоения дисциплины обучающийся должен:
Знать: нормативные правовые акты, методические документы и национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; процедуру организации установки и настройки технических, программных (программ-но-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах; организационные меры 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; разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации; анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей без-опасности информации в автоматизированных системах; вести протоколы и журналы учёта при осуществлении аудита систем защиты информации автоматизированных систем
Владеть: навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации; навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации; навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы

По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины Аттестация объектов информатизации

по направлению подготовки 10.03.01 Информационная безопасность

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата