Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки/ В	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
4	2	72	8	0	22		42	0	З
Итого	2	72	8	0	22	12	42	0	

Москва, 2020

АННОТАЦИЯ

Рабочая программа учебной дисциплины «Сертификация средств защиты информации по требованиям безопасности информации» содержит описание целей освоения дисциплины, ее место в структуре ООП, ВО, формируемые в результате освоения дисциплины компетенции студента, структуру и содержание дисциплины, используемые во время освоения дисциплины образовательные технологии, оценочные средства для контроля успеваемости, учебно-методическое, информационное и материально-техническое обеспечение дисциплины.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями реализации учебной дисциплины «Сертификация средств защиты информации по требованиям безопасности информации» является получение компетенций, необходимых для осуществления профессиональной деятельности, в части организации и проведения работ по сертификации средств защиты информации по требованиям безопасности информации.

Студенты по настоящей программе готовятся к осуществлению следующих видов деятельности: организационно-управленческая, проектная и эксплуатационная.

Объектами освоения дисциплины являются:

- средства защиты информации, средства контроля ее защищенности, а также средства, в которых они реализованы, подлежащие обязательной сертификации в сфере компетенции ФСТЭК России;
- система нормативных правовых актов, методических документов и национальных стандартов в области сертификации средств защиты информации.

Задачами дисциплины являются:

а) в организационно-управленческой деятельности:

- организация проведения сертификационных испытаний средств защиты информации;
- организация деятельности испытательной лаборатории и органа по сертификации;
- осуществление взаимодействия с заявителями, другими лабораториями и органами по сертификации (включая выбор испытательной лаборатории в соответствии с областью ее аккредитации, определение схемы сертификации,
- отбор образцов, согласование и утверждение программ и методик испытаний и т.д.);
- организация аттестации производства сертифицированных средств защиты информации;

б) в проектной деятельности:

- оказание консультативной и методической помощи по вопросам создания и сертификации средств защиты информации;
- разработка программы и методики сертификационных испытаний с учетом схемы сертификации;
- определение и уточнение требований безопасности информации к средствам защиты информации;
- разработка предложений по актуализации фонда и совершенствованию нормативных актов и методических документов, необходимых для проведения сертификации средств защиты информации;

в) в эксплуатационной деятельности:

- разработка документов по результатам сертификации и сертификационных испытаний средств защиты информации;

- проведение экспертизы документации, а также материалов сертификационных испытаний, оформление экспертного заключения по ее результатам;

- проведение сертификационных испытаний средств защиты информации, оформление протоколов и технических заключений по их результатам;

- проведение аттестации производства сертифицированных средств защиты информации;

- маркирование и контроль маркирования сертифицированных средств защиты информации;

- проведение инспекционного контроля сертифицированных средств защиты информации.

Дисциплина «Сертификация средств защиты информации по требованиям безопасности информации» является неотъемлемой составной частью профессиональной подготовки магистров по образовательной программе подготовки «Обеспечение безопасности значимых объектов критической информационной инфраструктуры». Вместе с другими дисциплин специального цикла изучение данной дисциплины призвано вырабатывать такие качества, как:

- строгость в суждениях,
- творческое мышление,
- организованность и работоспособность,
- дисциплинированность,
- самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Сертификация средств защиты информации по требованиям безопасности информации» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико-математической подготовкой, знаниями, умениями и навыками смежных дисциплин «Электротехника», «Метрология и электрорадиоизмерения», «Основы радиотехники», «Распространение радиоволн», «Программно-аппаратные средства обеспечения информационной безопасности», «Антенно-фидерные устройства», «Физические основы технических каналов утечки информации», «Измерительная аппаратура анализа защищенности объектов», «Методы и средства контроля эффективности защиты информации от несанкционированного доступа», «Основы технической защиты конфиденциальной информации».

Знания, полученные при изучении дисциплины «Сертификация средств защиты информации по требованиям безопасности информации» являются базовыми, для дисциплин, входящих в вариативную часть профессионального цикла учебного плана подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность» по образовательной программе подготовки «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-2.3 [1] - Способен устанавливать требования к обеспечению безопасности значимого объекта КИИ, осуществлять выбор и реализацию мер по обеспечению безопасности значимых объектов КИИ *Основание:* Профессиональный стандарт: 06.033, 06.034	З-ПК-2.3[1] - Знать: Отечественные стандарты в области информатизации и обеспечения информационной безопасности АСУ, информационных и телекоммуникационных систем общего и специального назначения; Основные принципы обеспечения безопасности КИИ; Основные положения ядерной безопасности; Причины возникновения инцидентов ядерной безопасности; Основные виды угроз для АСУ ТП на АЭС; Сущность основных физических процессов и информационных угроз в АСУ ТП в ядерном реакторе, их взаимосвязь; Требования по обеспечению безопасности значимых объектов КИИ.; У-ПК-2.3[1] - Уметь: Планировать, разрабатывать,

			совершенствовать и осуществлять внедрение мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Выявлять основные информационные угрозы в АСУ ТП ядерного реактора; Проводить оценку необходимости применения средств ядерной защиты реакторов. ; В-ПК-2.3[1] - Владеть: Навыками внедрения мероприятий, регламентирующих правила и процедуры по обеспечению безопасности значимых объектов КИИ; Навыками внедрения мероприятий по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности значимых объектов КИИ; Навыком обоснованного выбора средств защиты информации и средств ядерной защиты реакторов с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также

			категории значимого объекта КИИ; Навыком общего/детального анализа структуры системы безопасности значимого объекта КИИ.
научно- исследовательский			
Анализ фундаментальных и прикладных проблем ИБ в условиях становления современного информационного общества; выполнение научных исследований в области ИБ; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях	Фундаментальные и прикладные проблемы информационной безопасности; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.030	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной

			безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.
контрольно-аналитический			
Контроль защищенности ЗО КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации	Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, обеспечивающие безопасность критических процессов значимых объектов критической информационной инфраструктуры	ПК-4 [1] - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.034	З-ПК-4[1] - Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы организации работ при проведении сертификации программно-

			аппаратных средств защиты; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие требованиям по безопасности информации. ; У-ПК-4[1] - Уметь: оценивать эффективность защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему с целью определения уровня защищенности и доверия; применять инструментальные средства проведения сертификационных испытаний; разрабатывать программы и методики сертификационных испытаний

			программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; проводить экспертизу технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4[1] - Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; основами подготовки протоколов испытаний и технического заключения по результатам сертификационных испытаний программных (программно-технических) средств

			защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	4 Семестр						
1	Организационно-правовые основы ТЗИ. Организация и проведение сертификации средств защиты информации по требованиям безопасности информации	1-8			25	КИ-8	З-ОПК-3, У-ОПК-3, З-ПК-2.3, У-ПК-2.3, З-ПК-3, У-ПК-3, З-ПК-4, У-ПК-4

2	Организация деятельности испытательных лабораторий и органов по сертификации	9-15			25	КИ-15	З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-2.3, У-ПК-2.3, В-ПК-2.3, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4, У-ПК-4, В-ПК-4
	Итого за 4 Семестр		8/0/22		50		
	Контрольные мероприятия за 4 Семестр				50	З	З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-2.3, У-ПК-2.3, В-ПК-2.3, З-ПК-3, У-ПК-3, В-

							ПК-3, З-ПК-4, У-ПК-4, В-ПК-4

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	4 Семестр	8	0	22
1-8	**Организационно-правовые основы ТЗИ. Организация и проведение сертификации средств защиты информации по требованиям безопасности информации**	4		12
1	**Тема 1. Цели и задачи технической защиты информации. Правовые основы ТЗИ. Организация работ по ТЗИ в организации. Способы и средства защиты информации. Средства контроля защищенности информации** Основные термины и определения в области ТЗИ. Государственная система противодействия иностранным техническим разведкам и ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ТЗИ. Объекты информатизации: классификация и характеристика. Организация научных исследований и разработок в области ТЗИ. Правовые основы защиты информации. Система документов в области ТЗИ. Нормативные правовые акты. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Общие требования по ТЗИ. Комплекс мероприятий по ТЗИ. Модели угроз и краткая характеристика угроз безопасности информации. Создание и функционирование	Всего аудиторных часов 2 Онлайн		

	системы защиты информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий. Требования и рекомендации по защите информации от несанкционированного доступа (НСД). Требования и рекомендации по защите речевой информации. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники (СВТ) от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН) Требования по обеспечению защиты информации при взаимодействии абонентов с информационными сетями общего пользования. Общие положения. Способы и средства защиты информации от НСД. Способы и средства защиты речевой информации. Способы и средства защиты информации, обрабатываемой СВТ от утечки за счет ПЭМИН. Основные задачи контроля эффективности ТЗИ. Общие требования, способы и средства контроля эффективности ТЗИ.			
2	**Тема 2. Документы, регламентирующие деятельность в области создания средств защиты информации и сертификации средств защиты информации. Процедура, технологические этапы и задачи сертификации средств з** Основные термины и определения в области сертификации. Цели сертификации. Объект сертификации в Системе сертификации ФСТЭК России и его признаки. Формы оценки соответствия и ключевые особенности обязательной сертификации. Системы сертификации средств защиты информации по требованиям безопасности информации в федеральных органах исполнительной власти. Организационная структура системы сертификации ФСТЭК России, задачи и функции ее участников. Система документов по сертификации средств зашиты информации в Системе сертификации России. Документы технического регулирования стандартизации, применяемые при производстве и сертификации средств защиты информации. Реестр сертифицированных средств защиты информации. Схемы обязательной сертификации. Процедуры первичной сертификации средств защиты информации, продления сертификата, аннулирования или приостановки действия сертификата, выдачи сертификата соответствия, подачи и рассмотрения апелляций. Задачи сертификационных испытаний! Подготовка заявки на сертификацию. Идентификация средств защиты информации. Отбор образцов для проведения испытаний. Инженерный анализ. Классификация и типизация средств защиты информации. Требования к составу и содержанию документации средств защиты информации при проведении их сертификации. Требования безопасности информации к средствам защиты информации, дифференциация и взаимосвязь требований.	Всего аудиторных часов 2 Онлайн		

	Источники задания требований и взаимосвязь требований документов ФСТЭК России, требований документов разработчика средства защиты информации и ограничений на эксплуатацию. Требования к структуре и содержанию технических условий и паспорта (формуляра). Требования к структуре и содержанию задания по безопасности. Терминология, структура, зависимости и операции над компонентами функциональных требований безопасности информации по ГОСТ Р ИСО/МЭК 15408-2. Анализ результатов испытаний и разработка ограничений на эксплуатацию.			
3	**Тема 3. Разработка программ и методик сертификационных испытаний. Требования к содержанию и оформлению. Методы испытаний.** Классификация и описание основных методов сертификационных испытании средств защиты информации. Общие требования к программам и методикам испытаний по ГОСТ В 15.211. Методология оценки по ГОСТ Р ИСО/МЭК 18045, оценка задания по безопасности, оценка путем тестирования, взаимосвязь тестирования разработчика и независимого тестирования. Структура, содержание, порядок разработки и согласования программ и методик испытаний.	Всего аудиторных часов		
				2
		Онлайн		
4	**Тема 4. Типовые сертификационные испытания программных и аппаратных средств защиты информации.** Порядок испытаний средств защиты информации от НСД. Контроль отсутствия недекларированных возможностей. Особенности использования исходных текстов и объектных сторонних разработчиков. Анализ уязвимостей средств защиты информации от НСД, источники и банки данных по уязвимостям средств защиты информации от НСД. Порядок испытаний средств защиты информации от утечки по техническим каналам. Физические основы возникновения и характеристика технических каналов утечки информации (ТКУИ). Основные виды физико-технических измерений при испытаниях средств защиты информации от утечки по техническим каналам. Требования к документам, оформляемым по результатам сертификационных испытаний. Порядок проведения экспертизы результатов сертификационных испытаний.	Всего аудиторных часов		
				2
		Онлайн		
5	**Тема 5. Инструментальное обеспечение сертификационных испытаний. Типовые контрольно-измерительная аппаратура и лабораторное оборудование.** Единство измерений и его обеспечение. Метрологическое обеспечение сертификационных испытаний. Обязательная поверка и калибровка. Номенклатура средств измерений, подлежащих поверке. Инструментальное обеспечение сертификационных испытаний. Особенности проведения испытаний на материальной базе заявителя. Возможности и характеристики типовой контрольно-измерительной	Всего аудиторных часов		
				2
		Онлайн		

	аппаратуры, лабораторного оборудования. Возможности и характеристики программных средств активного аудита и анализа защищенности.			
6	**Тема 6. Меры обеспечения достоверности и качества результатов испытаний. Метрологическое обеспечение испытаний.** Основные понятия метрологии, погрешности измерений Воспроизводимость и повторяемость результатов. Метрологическое обеспечение сертификационных испытаний. Общие требования к измерениям. Анализ постановки измерительной задачи. Обработка результатов измерений. Требования к методам обработки прямых многократных измерений, обработки нормально распределенных данных, обработки данных, распределение которых отлично от нормального, обработки результатов косвенных измерений. Меры обеспечения достоверности испытаний продуктов информационных технологий. Компоненты доверия по ГОСТ Р ИСО/МЭК 15408-3 к свидетельствам разработчика (документация средств защиты информации, тесты разработчика). Компоненты доверия на основе независимых оценок (независимое тестирование, анализ уязвимостей).	Всего аудиторных часов		
				2
		Онлайн		
7	**Тема 7. Цели, задачи, порядок проведения аттестации производства. Система качества организации.** Технология проведения аттестации производства. Порядок организации системы производственного контроля на предприятии. Процессный подход ГОСТ Р ИСО 9001-2015 и процессы жизненного цикла средств защиты информации. Порядок проведения аттестации производства, его цели и задачи. Организация технологического процесса и технологическая документация производства изделия, организация входного и выходного контроля. Требования по учету произведенной сертифицированной продукции, требования к системе послепродажного обслуживания, учета и отработки рекламаций.	Всего аудиторных часов		
				2
		Онлайн		
8	**Тема 8. Программа и методика проведения аттестации производства. Порядок оформления акта аттестации производства.** Требования к содержанию программ и методик аттестации производства. Оценка достаточности производственных испытаний для обеспечения неизменности сертифицированных характеристик средств защиты информации. Порядок оформления акта аттестации производства.	Всего аудиторных часов		
				2
		Онлайн		
9-15	**Организация деятельности испытательных лабораторий и органов по сертификации**	4		10
9	**Тема 9. Организация деятельности испытательных лабораторий и органов по сертификации** Принципы независимости, беспристрастности, конфиденциальности и раскрытия информации в деятельности испытательной лаборатории. Порядок	Всего аудиторных часов		
		2		2
		Онлайн		

	аккредитации испытательных лабораторий и органов по сертификации аккредитационные требования и условия. Система организационно-распорядительных документов испытательных лабораторий и органов по сертификации. Условия хранения образцов средств защиты информации в испытательной лаборатории. Ответственность за результаты сертификации и сертификационных испытаний. Определение (расчет) трудозатрат и стоимости проведения работ по сертификации средств защиты информации.			
10 - 11	**Тема 10. Система внутреннего документооборота испытательных лабораторий и органов по сертификации** Система документов и порядок ведения внутреннего документооборота испытательных лабораторий и органов по сертификации. Правовое обеспечение сохранности государственной тайны и авторских прав. Требования и порядок обеспечения режима секретности при проведении сертификации средств защиты информации и оформлении материалов испытаний. Требования и порядок соблюдения авторских прав при проведении сертификации средств защиты информации. Порядок хранения документации и материалов сертификации средств защиты информации в испытательной лаборатории и органе по сертификации.	Всего аудиторных часов		
		2		2
		Онлайн		
12 - 13	**Тема 11. Система менеджмента качества и информационной безопасности испытательных лабораторий и органов по сертификации** Требования международных и национальных стандартов Российской Федерации в области менеджмента качества и информационной безопасности. Модель системы менеджмента качества, основанной на процессном подходе. Организация системы менеджмента качества и политики информационной безопасности испытательных лабораторий и органов по сертификации. Сертификация системы менеджмента качества и политики информационной безопасности испытательных лабораторий и органов по сертификации.	Всего аудиторных часов		
				2
		Онлайн		
14	**Тема 12. Организация и проведение инспекционного контроля сертифицированных средств защиты информации. Порядок внесения изменений средства защиты информации** Порядок внесения изменений в технические средства защиты информации, программные средства защиты информации, документация средств защиты информации и технологию производства средств защиты информации. Порядок документирования изменений.	Всего аудиторных часов		
				2
		Онлайн		
15	**Тема 13. Порядок проведения инспекционного контроля сертифицированных средств защиты информации. Продление сертификата соответствия средств защиты информации владельцем объекта информатизации** Порядок продления сертификата соответствия средств защиты информации заявителем. Порядок проведения	Всего аудиторных часов		
				2
		Онлайн		

	инспекционного контроля. Регистрация и выдача знаков соответствия, маркирование сертифицированных средств защиты информации. Порядок продления сертификата соответствия организацией, эксплуатирующей средства защиты информации.			

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	4 Семестр
4 - 5	**Лабораторная работа № 1.** Проведение инженерного анализа средств защиты информации и экспертизы документации программных и аппаратных средств защиты информации от НСД
6 - 8	**Лабораторная работа № 2.** Проведение инженерного анализа средств защиты информации и экспертизы документации программных и аппаратных средств защиты информации от утечки по техническим каналам
9 - 10	**Лабораторная работа № 3.** Проведение основных видов функциональных проверок средств защиты информации от НСД по требованиям безопасности информации с применением программных средств контроля
11 - 14	**Лабораторная работа № 4.** Проведение основных видов физико-технических измерений при испытаниях средств защиты информации от утечки по техническим каналам с применением средств измерений

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий.

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные,

нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по отработке программно-аппаратных средств выявления угроз безопасности информации, обусловленных несанкционированным доступом к ней, проводится в специализированной лаборатории с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла лабораторных работ выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении лабораторных работ необходимо отрабатывать задания, в том числе с проведением деловых игр (эпизодов).

Лабораторные работы по аттестации объектов информатизации по требованиям безопасности информации, обнаружению ТКУИ и отработке методического аппарата технического контроля проводятся по циклам на автоматизированных рабочих местах в специализированных лабораториях. На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое оборудование технического контроля и средства имитации ТКУИ. Результаты, полученные в ходе лабораторных работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ПК-2.3	З-ПК-2.3	З, КИ-8, КИ-15
	У-ПК-2.3	З, КИ-8, КИ-15
	В-ПК-2.3	З, КИ-15
ПК-3	З-ПК-3	З, КИ-8, КИ-15
	У-ПК-3	З, КИ-8, КИ-15
	В-ПК-3	З, КИ-15
ПК-4	З-ПК-4	З, КИ-8, КИ-15
	У-ПК-4	З, КИ-8, КИ-15

	В-ПК-4	З, КИ-15

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

2. ЭИ К65 Контроль защищенности автоматизированных систем от несанкционированного доступа. Аттестационные испытания : лабораторный практикум, Москва: НИЯУ МИФИ, 2013

3. ЭИ Д84 Оценка защищенности речевой информации Ч.1 Выявление акустических и вибрационных каналов утечки речевой информации, Москва: НИЯУ МИФИ, 2015

4. ЭИ Д84 Оценка защищенности речевой информации Ч.2 Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования, Москва: НИЯУ МИФИ, 2015

5. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале акустоэлектромагнитного преобразования, Москва: НИЯУ МИФИ, 2018

6. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале высокочастотного акустоэлектрического преобразования, Москва: НИЯУ МИФИ, 2015

7. ЭИ Д84 Оценка защищенности речевой информации Ч.4 Проведение инструментального контроля в канале высокочастотного навязывания, Москва: НИЯУ МИФИ, 2018

8. ЭИ Д84 Оценка защищенности речевой информации Ч.5 Проведение инструментального контроля в канале высокочастотного облучения, Москва: НИЯУ МИФИ, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы - Комплексная защита объектов информатизации, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Аттестация по разделам:

К8, КИ16 - максим.балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

При не аттестации хотя бы по одному из разделов, студент не допускается к зачету.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по отработке программно-аппаратных средств выявления угроз безопасности информации, обусловленных несанкционированным доступом к ней, проводится в специализированной лаборатории с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла лабораторных работ выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении лабораторных работ необходимо отрабатывать задания, в том числе с проведением деловых игр (эпизодов).

Лабораторные работы по сертификации средств защиты информации по требованиям безопасности информации, обнаружению ТКУИ и отработке методического аппарата технического контроля проводятся по циклам на автоматизированных рабочих местах в специализированных лабораториях. На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое оборудование технического контроля и средства имитации ТКУИ. Результаты, полученные в ходе лабораторных работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы - «Обеспечение безопасности значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

Аттестация по разделам:

КР8, КИ16 - максим. балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

При неаттестации хотя бы по одному из разделов, студент не допускается к экзамену.

1. Чтение лекций.

Первая лекция должна быть введением к дисциплине (разделу дисциплины, читаемому

в начинающемся семестре). Она должна содержать общий обзор содержания дисциплины. В ней следует отметить методические инновации в решении задач, рассматриваемых в дисциплине, дать перечень рекомендованной литературы и вновь появившихся литературных источников, обратив внимание студентов на обязательную и дополнительную литературу.

Изложению текущего лекционного материала должна предшествовать вводная часть, содержащая краткий перечень вопросов, рассмотренных на предыдущих лекциях. На этом этапе полезно задать несколько вопросов аудитории, осуществить выборочный контроль знания студентов.

При изложении лекционного материала следует поощрять вопросы непосредственно в процессе изложения, внимательно относясь к вопросам студентов и при необходимости давая дополнительные, более подробные пояснения.

При чтении лекций преимущественное внимание следует уделять качественным вопросам, опуская простые математические выкладки, либо рекомендуя выполнить их самим студентам, либо отсылая студентов к литературным источникам и методическим пособиям.

В процессе лекционного курса необходимо возможно чаще возвращаться к основным вопросам дисциплины, проводя выборочный экспресс-контроль знаний студентов.

Принятая преподавателем система обозначений должна чётко разъясняться в процессе её введения и использоваться в конспектах лекций

В лекциях, предшествующих практическим занятиям, следует кратко излагать содержание и основные задачи практического занятия, дать рекомендации студентам для подготовки к нему.

На последней лекции важно найти время для обзора основных положений, рассмотренных в дисциплине, перечню и формулировке вопросов, выносимых на экзамен или зачёт.

2. Указания по контролю самостоятельной работы студентов.

По усмотрению преподавателя задание на самостоятельную работу может быть индивидуальным или фронтальным.

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе, проводить его обсуждение.

При применении фронтальных заданий вести коллективные обсуждения со студентами основных теоретических положений.

С целью контроля качества выполнения самостоятельной работы требовать индивидуальные отчеты (допустимо вместо письменного отчета применять индивидуальные контрольные вопросы).

Автор(ы):

Дураковский Анатолий Петрович, к.т.н., доцент

Рецензент(ы):

Горбатов В.С.