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

ОСНОВЫ КАТЕГОРИРОВАНИЯ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

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**
2	2	72	8	22	0		42	0	З
Итого	2	72	8	22	0	2	42	0	

Москва, 2020

АННОТАЦИЯ

Рабочая программа учебной дисциплины «Основы категорирования значимых объектов критической информационной инфраструктуры» содержит описание целей освоения дисциплины, ее место в структуре ООП, 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 освоения учебной дисциплины являются обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ аттестации защищаемых помещений по требованиям безопасности информации. Дисциплина «Основы категорирования значимых объектов критической информационной инфраструктуры» имеет целью обучить студентов (слушателей) основным принципам построения и технологиям, используемых в настоящее время при создании подсистем обеспечения безопасности значимых объектов критической информационной инфраструктуры, рекомендованных международными организациями по стандартизации в области ИБ и российскими нормативными актами, и стандартами. Курс позволяет дать понятие студентам основные представления об основах категорирования значимых объектов критической информационной инфраструктуры.

Задачами дисциплины являются:

- дать основы правовых, организационно-распорядительных, нормативных и информационных документов в области ОБЗОКИИ; организации и порядка проведения категорирования ЗО КИИ и отработки документов по результатам категорирования.

В результате обучения студенты должны ознакомиться с:

системой организационно-распорядительных, нормативных и информационных документов ФСТЭК России и Ростехрегулирования, определяющих организацию, правила и порядок осуществления категорирования ЗО КИИ;

организацией лицензирования деятельности в области защиты информации,

организацией контроля выполнения требований федерального законодательства и приказов ФСТЭК России;

должны знать:

организационно-технические основы категорирования ЗО КИИ;

должны уметь:

проводить специальные категорирование ЗО КИИ;

должны владеть навыками:

выявления критических процессов на ЗО КИИ;

разработки технических документов по результатам категорирования ЗО КИИ.

Дисциплина «Основы категорирования значимых объектов критической информационной инфраструктуры» 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 «Основы категорирования значимых объектов критической информационной инфраструктуры» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

Знания, полученные при изучении дисциплины «Основы категорирования значимых объектов критической информационной инфраструктуры» 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-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.030,	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и

		06.032, 06.033, 06.034	защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать

			защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации

			(модели угроз безопасности информации).
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-2.1 [1] - Способен определять объекты КИИ, готовить перечни объектов КИИ, подлежащие категорированию *Основание:* Профессиональный стандарт: 06.030, 06.034	З-ПК-2.1[1] - Знать: Основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов; Принципы построения АСУ ТП АЭС и критические процессы, происходящие в результате штатной работы. ; У-ПК-2.1[1] - Уметь: Выявлять и собирать сведения о критических процессах в АСУ, информационных и телекоммуникационных системах, в частности в АСУ ТП АЭС; Определять категории значимости объектов КИИ; Формировать сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. ; В-ПК-2.1[1] - Владеть: Навыком определения критических процессов в АСУ, информационных и телекоммуникационных системах, в частности в АСУ ТП АЭС; Навыком определения категории значимости

			объектов КИИ; Навыком формирования сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.
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-2.2 [1] - Способен осуществлять категорирование объектов КИИ и готовить сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий *Основание:* Профессиональный стандарт: 06.030, 06.032	З-ПК-2.2[1] - Знать: Процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ; Последствия инцидентов информационной и ядерной безопасности; Процедуру подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. ; У-ПК-2.2[1] - Уметь: Разрабатывать необходимые документы, содержащие сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для направления в федеральный орган исполнительной власти, уполномоченный в

			области обеспечения безопасности КИИ, по утвержденной им форме. ; В-ПК-2.2[1] - Владеть: Навыком анализа последствий инцидентов информационной и ядерной безопасности; Навыком категорирования объектов КИИ.
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.
организационно-управленческий			
Организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры	Контроль защищенности информации на объектах информатизации	ПК-2.4 [1] - Способен обеспечивать безопасность значимого объекта КИИ на всех стадиях жизненного цикла *Основание:* Профессиональный стандарт: 06.031, 06.033, 06.034	З-ПК-2.4[1] - Знать: Принципы организации систем безопасности значимых объектов КИИ и обеспечения их функционирования; Критерии обеспечения ядерной безопасности значимых объектов КИИ.; У-ПК-2.4[1] - Уметь: Анализировать данные, получаемые при использовании средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе информации о наличии в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, признаков компьютерных атак.; В-ПК-2.4[1] - Владеть: Навыком проведения перспективных исследований в области информационной безопасности и ядерной защиты объектов КИИ; Навыком совершенствования системы безопасности значимых объектов КИИ; Навыком управления (администрирования) системой безопасности

			и реагирования на компьютерные инциденты; Навыком проведения контроля состояния (мониторинг) критических процессов и системы безопасности значимого объекта КИИ.
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
	2 Семестр						
1	Общие положения законодательной и нормативно- правовой базы в области обеспечения безопасности значимых объектов критической информационной инфраструктуры	1-8			25	КИ-8	З-ПК-1, У-ПК-1, З-ПК-2.1, У-ПК-2.1, З-ПК-2.2, У-ПК-2.2, З-ПК-2.3, У-ПК-2.3, З-ПК-

							2.4, У-ПК-2.4, З-ПК-4, У-ПК-4
2	Организация и проведение работ категорированию значимых объектов КИИ	9-15			25	КИ-15	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2.1, У-ПК-2.1, В-ПК-2.1, З-ПК-2.2, У-ПК-2.2, В-ПК-2.2, З-ПК-2.3, У-ПК-2.3, В-ПК-2.3, З-ПК-2.4, У-ПК-2.4, В-ПК-2.4, З-ПК-4, У-ПК-4, В-ПК-4

	Итого за 2 Семестр		8/22/0		50		
	Контрольные мероприятия за 2 Семестр				50	З	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2.1, У-ПК-2.1, В-ПК-2.1, З-ПК-2.2, У-ПК-2.2, В-ПК-2.2, З-ПК-2.3, У-ПК-2.3, В-ПК-2.3, З-ПК-2.4, У-ПК-2.4, В-ПК-2.4, 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:

Обозна	**Полное наименование**

чение	
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	2 Семестр	8	22	0
1-8	**Общие положения законодательной и нормативно-правовой базы в области обеспечения безопасности значимых объектов критической информационной инфраструктуры**	4	12	
1 - 2	**Тема 1. Правовые основы обеспечения безопасности КИИ Российской Федерации** Тема 1. Правовые основы обеспечения безопасности КИИ Российской Федерации Правовые основы обеспечения безопасности КИИ Российской Федерации. Объекты и субъекты КИИ. Права и обязанности субъектов КИИ. Особенности обеспечения безопасности объектов КИИ Российской Федерации. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ. Система безопасности значимого объекта КИИ. Права и обязанности субъектов критической информационной инфраструктуры. Государственный контроль в области обеспечения безопасности значимых объектов КИИ. Цели государственного контроля в области обеспечения безопасности значимых объектов КИИ. Виды и периодичность государственного контроля. Основание для проведения плановых и внеплановых проверок. Система нормативных правовых актов по вопросам обеспечения безопасности КИИ Российской Федерации. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Организационно-правовые основы лицензирования деятельности в области защиты информации, аттестации объектов информатизации по требованиям безопасности информации. Система сертификации средств защиты информации. Ответственность за нарушение законодательства о безопасности КИИ Российской Федерации.	Всего аудиторных часов 1 Онлайн	4	
3 - 4	**Тема 2. Угрозы безопасности информации, обрабатываемой на объектах КИИ**	Всего аудиторных часов 1	4	

	Объекты КИИ. Объекты защиты. Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении значимых объектов КИИ. Модель угроз безопасности информации значимого объекта КИИ. Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз безопасности информации и их последствия. Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Типовые способы реализации угроз для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Типовые компьютерные инциденты для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности информации и последствий от их реализации. Объекты оценки уязвимости: код, конфигурация и архитектура значимого объекта КИИ для всех программных и программно-аппаратных средств, в том числе средств защиты информации значимого объекта КИИ. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.	Онлайн		
5 - 8	**Тема 3 Организация работ по обеспечению безопасности значимого объекта КИИ** Тема 2. Угрозы безопасности информации, обрабатываемой на объектах КИИ Объекты КИИ. Объекты защиты. Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении значимых объектов КИИ. Модель угроз безопасности информации значимого объекта КИИ. Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз безопасности информации и их последствия. Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.	Всего аудиторных часов 2 Онлайн	4	

	Типовые способы реализации угроз для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Типовые компьютерные инциденты для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности информации и последствий от их реализации. Объекты оценки уязвимости: код, конфигурация и архитектура значимого объекта КИИ для всех программных и программно-аппаратных средств, в том числе средств защиты информации значимого объекта КИИ. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ. Тема 3 Организация работ по обеспечению безопасности значимого объекта КИИ Установление требований по обеспечению безопасности значимого объекта КИИ. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ. Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения плана мероприятий по обеспечению безопасности значимого объекта КИИ. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ. Организационные и технические меры, направленные на блокирование (нейтрализацию) угроз безопасности информации: идентификация и аутентификация; управление доступом; ограничение программной среды; защита машинных носителей информации; аудит безопасности; антивирусная защита; предотвращение вторжений (компьютерных атак); обеспечение целостности; обеспечение доступности; защита технических средств и систем; защита информационной (автоматизированной) системы (сети) и ее компонентов; реагирование на инциденты информационной безопасности; управление конфигурацией; управление обновлениями программного обеспечения; планирование мероприятий по обеспечению безопасности;			

	обеспечение действий в нештатных (непредвиденных) ситуациях; информирование и обучение персонала. Выбор организационных и технических мер для обеспечения безопасности значимых объектов КИИ. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности. Требования к классам защиты средств защиты информации и средствам вычислительной техники для различных категорий значимости объектов КИИ. Нормативные правовые акты ФСТЭК России, в соответствии с которыми определяются классы защиты средств защиты информации и средств вычислительной техники. Функции безопасности средств защиты информации. Программа и методики испытаний (приемки) средств защиты информации, утверждаемые субъектом КИИ.			
9-15	**Организация и проведение работ категорированию значимых объектов КИИ**	4	10	
9 - 12	**Тема 4. Требования по обеспечению безопасности значимых объектов КИИ** Правила и порядок категорирования объектов КИИ, сроки направления сведений о результатах категорирования объекта КИИ в ФСТЭК России. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ. Формирование комиссии по категорированию объектов КИИ Российской Федерации. Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов. Определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ Российской Федерации. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (критических процессов). Анализ возможных действий нарушителей в отношении объектов КИИ. Анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объекте КИИ. Оценка возможных последствий компьютерных инцидентов на объектах КИИ.	Всего аудиторных часов 2 Онлайн	6	

	Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значения. Формирование перечня объектов КИИ Российской Федерации, подлежащих категорированию. Оценка в соответствии с перечнем показателей критериев значимости объектов КИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ Российской Федерации Присвоение объектам КИИ Российской Федерации одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости. Подготовка необходимых документов в рамках категорирования объектов КИИ Российской Федерации.			
13 - 15	**Тема 5. Система безопасности значимого объекта КИИ** Цели и задачи системы безопасности значимого объекта КИИ. Требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования. Требования к силам обеспечения безопасности значимых объектов КИИ. Требования к организационно-распорядительным документам по безопасности значимых объектов КИИ. Структура системы безопасности значимого объекта КИИ. Подготовка необходимых документов в рамках создания систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования. Этапы жизненного цикла системы безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности значимого объекта КИИ. Тестирование функционирования системы безопасности значимого объекта КИИ и макетирование элементов системы. Разработка эксплуатационной, организационно-распорядительной документации на значимый объект КИИ и его систему безопасности. Внедрение системы безопасности значимого объекта КИИ. Установка и настройка средств защиты информации. Разработка документов по безопасности значимого объекта КИИ. Внедрение организационных мер по обеспечению безопасности значимого объекта КИИ. Предварительные испытания значимого объекта КИИ и его системы безопасности. Опытная эксплуатация значимого объекта КИИ и его системы безопасности. Приемочные испытания значимого объекта КИИ и его системы безопасности. Заключение.	Всего аудиторных часов		
		2	4	
		Онлайн		

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 ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	2 Семестр
	Тема 1 Разработка модели угроз безопасности информации значимого объекта КИИ
	Тема 2 Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности
	Тема 3 Определение значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов
	Тема 4 Формирование акта комиссии по категорированию значимого объекта КИИ
	Тема 5 Подготовка сведений о результатах категорирования значимого объекта КИИ
	Тема 6 Разработка плана мероприятий по обеспечению безопасности значимого объекта КИИ
	Тема 7 Разработка правил и порядка реализации отдельных мер по обеспечению безопасности значимых объектов КИИ
	Тема 8 Разработка технического задания (разделов технического задания) на создание системы безопасности значимого объекта КИИ

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 категорированию значимых объектов критической информационной инфраструктуры. 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 практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Результаты 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-1	З-ПК-1	З, КИ-8, КИ-15
	У-ПК-1	З, КИ-8, КИ-15
	В-ПК-1	З, КИ-15
ПК-2.1	З-ПК-2.1	З, КИ-8, КИ-15
	У-ПК-2.1	З, КИ-8, КИ-15
	В-ПК-2.1	З, КИ-15
ПК-2.2	З-ПК-2.2	З, КИ-8, КИ-15
	У-ПК-2.2	З, КИ-8, КИ-15
	В-ПК-2.2	З, КИ-15
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-2.4	З-ПК-2.4	З, КИ-8, КИ-15
	У-ПК-2.4	З, КИ-8, КИ-15
	В-ПК-2.4	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 П 84 Информационная безопасность и защита информации : учебное пособие, Санкт-Петербург: Лань, 2021

2. ЭИ Н 62 Методы защиты информации. Защита от внешних вторжений : учебное пособие для вузов, Санкт-Петербург: Лань, 2020

3. ЭИ П 54 Организационное и правовое обеспечение информационной безопасности : Учебник и практикум для вузов, Москва: Юрайт, 2021

4. ЭИ Н 56 Основы информационной безопасности : учебное пособие, Санкт-Петербург: Лань, 2019

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, место курса в различных областях науки и техники, в том числе в области информационной безопасности.

Аттестация по разделам:

КР8, КР16 - максим.балл - 25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех практических заданий 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. 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 практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений.

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 практических занятиях.

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, место курса в различных областях науки и техники, в том числе в области информационной безопасности.

Аттестация по разделам:

КР8, КР16 - 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.

Чтение лекций.

Теоретическая часть материала темы отрабатывается на лекциях и практических занятиях. На лекционных занятиях излагаются наиболее важные и сложные учебные вопросы, являющиеся фундаментальной основой нормативной базы и практических рекомендаций в области обеспечения безопасности значимых объектов КИИ. Часть лекций излагается проблемным методом с привлечением обучающихся для решения сформулированной преподавателем задачи.

Практические занятия проводятся с целью углубления и закрепления знаний на конкретных примерах из практики, обсуждения частных случаев, важных для освоения вопросов темы, а также привития навыков поиска и анализа учебной информации, умения участвовать в дискуссии по вопросам обеспечения безопасности значимых объектов КИИ.

На практических занятиях развиваются умения и навыки выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, разработки организационно-распорядительных документов по безопасности значимых объектов КИИ, а также установки, настройки и применения современных средств защиты информации, обрабатываемой объектами КИИ.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, выдаваемым в конце каждого занятия, с указанием отрабатываемых учебных вопросов, учебно-методического и информационного обеспечения.

Самостоятельная работа проводится в следующих формах: систематическая отработка лекционного материала, подготовка к семинарам, практическим занятиям, лабораторным работам и подготовка к итоговой аттестации.

С целью текущего контроля знаний в ходе занятий необходимо использовать различные приемы тестирования и контроля успеваемости обучающихся.

На изучение теоретических вопросов учебного модуля (темы) отводится 70 % учебного времени, практических - 30 %.

Автор(ы):

Резниченко Сергей Анатольевич

Рецензент(ы):

Дураковский А.П.