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

СИСТЕМЫ БЕЗОПАСНОСТИ 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**
4	2	72	8	22	0		42	0	З
Итого	2	72	8	22	0	12	42	0	

Москва, 2022

АННОТАЦИЯ

Главной целью преподавания дисциплины является обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ в области выбора и применения систем безопасности значимых объектов критической информационной инфраструктуры. При противодействии реализации информационных угроз значимому объекту КИИ помимо общего комплекса работ по выработке и поддержке грамотных управленческих решений на основе системного подхода специалисты-эксперты должны обладать дополнительными углубленными умениями и практическими навыками по целому ряду направлений, причем, каждое из них предполагает решение ряда частных и специфичных задач, требующих от специалиста-системника определенных умений и практических навыков, в том числе по применению специализированных программных средств и методов защиты критических процессов в указанных системах.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Системы безопасности значимых объектов критической информационной инфраструктуры» (далее — «Дисциплина») является формирование у студентов навыков самостоятельного планирования, организации и проведения работ по определению критических процессов и категорированию значимых объектов критической информационной инфраструктуры с помощью систем безопасности.

Основой является теоретическая и практическая подготовка студентов к деятельности, связанной с организацией работ по выбору специальных систем безопасности значимых объектов КИИ с помощью.

Задачами дисциплины являются:

- ознакомление с правовыми, организационно-распорядительными, нормативными и информационными документами в области безопасности значимых объектов критической информационной инфраструктуры (ЗОКИИ);

-ознакомление с физическими основами реализации угроз безопасности информации на объекте информатизации и порядка их выявления;

-ознакомление с системным подходом применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры и правилами выбора их систем безопасности;

-ознакомление с методиками проведения категорирования значимых объектов в соответствии с методологией исследований защищенности средств и систем на соответствие требованиям по безопасности информации;

-ознакомление с практикой отработки методик проведения категорирования значимого объека в соответствии с методологией исследований защищенности средств и систем на соответствие требованиям по безопасности информации;

-организация и порядок проведения аттестации объекта информатизации и отработка технической документации (ТД) по результатам испытаний на объектах КИИ.

В результате обучения студенты должны:

ознакомиться с:

системным подходом в обеспечении безопасности ЗОКИИ и правилами выбора систем безопасности ЗОКИИ

системой организационно-распорядительных, нормативных и информационных документов ФСТЭК России и Ростехрегулирования, определяющих организацию, правила и порядок осуществления деятельности в области защиты значимых объектов КИИ;

организацией контроля выполнения лицензионных требований и условий предприятиями-лицензиатами ФСТЭК России.

иметь представление:

о государственной системе защиты информации, ее задачах и структуре;

о правовых основах обеспечения информационной безопасности значимых объектов субъектов КИИ;

о защите (системный подход) в обеспечении безопасности ЗОКИИ и правилами выбора систем безопасности ЗОКИИ

знать:

основные понятия и требования предъявляемые к системе защиты ЗОКИИ;

организационно-технические основы категорирования ЗО КИИ;

основные методы защиты критических процессов ЗОКИИ;

уметь:

выбирать системы защиты ЗОКИИ;

выделять основания и объекты защиты, определять критические процессы и делать выбор систем защиты ЗОКИИ;

владеть навыками:

выявления критических процессов на ЗО КИИ;

разработки технических документов по результатам категорирования ЗО КИИ.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Данная учебная дисциплина входит в базовую часть профессионального модуля ООП «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» ОС НИЯУ МИФИ 10.04.01 «Информационная безопасность».

Изучение дисциплины предполагает предварительное освоение следующих дисци-плин учебного плана:

1. Физические основы технических каналов утечки информации;
2. Целенаправленные атаки на компьютерные системы
3. Основы информационной безопасности критически важных объектов;
4. Основы кибербезопасности атомной энергетики;
5. Основы категорирования значимых объектов критической информационной инфраструктуры;
6. Методы и средства контроля эффективности защиты информации от несанкционированного доступа;

Требования к «входным» знаниям, умениям и готовностям студента, необходимым при освоении данной дисциплины:

знать потенциальные угрозы безопасности информации значимых объетов субъектов КИИ;

уметь использовать системный подход, математический аппарат;

владеть основами физики, электротехники, измерений, радиотехники и выбора систем безопасности ЗОКИИ.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-1 [1] – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	З-ОПК-1 [1] – Знать: основы стандартов в области обеспечения информационной безопасности; элементы компьютерного моделирования сложных систем, проектирования информационных, автоматизированных и автоматических систем У-ОПК-1 [1] – Уметь: проектировать информационные системы; обосновывать и планировать состав и архитектуру моделируемых и проектируемых информационных, автоматизированных и автоматических систем; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности. В-ОПК-1 [1] – Владеть: навыками участия в разработке системы обеспечения информационной безопасности объекта; навыками проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности

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, 06.032, 06.033, 06.034	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 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	Средства и технологии обеспечения безопасности значимых	ПК-2.1 [1] - Способен определять объекты КИИ, готовить перечни объектов КИИ, подлежащие	З-ПК-2.1[1] - Знать: Основные принципы выявления объектов КИИ, которые обрабатывают

объектов на стадиях разработки, эксплуатации и модернизации	объектов критической информационной инфраструктуры	категорированию *Основание:* Профессиональный стандарт: 06.030, 06.034	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	Средства и	ПК-2.2 [1] - Способен	З-ПК-2.2[1] - Знать:

систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	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	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	Средства и технологии обеспечения	ПК-2.3 [1] - Способен устанавливать требования к	З-ПК-2.3[1] - Знать: Отечественные стандарты в области

безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	безопасности значимых объектов критической информационной инфраструктуры	обеспечению безопасности значимого объекта КИИ, осуществлять выбор и реализацию мер по обеспечению безопасности значимых объектов КИИ *Основание:* Профессиональный стандарт: 06.033, 06.034	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	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

инфраструктуры			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.

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	Раздел 1 Концепция и теоретические основы безопасности	1-8			25	КИ-8	З-ОПК-1,

	критической информационной инфраструктуры						У-ОПК-1, 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
2	Раздел 2 Системы безопасности значимых объектов критической информационной инфраструктуры	9-15			25	КИ-15	З-ОПК-1, У-ОПК-1, В-ОПК-1, 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
	Итого за 4 Семестр		8/22/0		50		
	Контрольные мероприятия за 4 Семестр				50	З	З-ОПК-1, У-ОПК-1, В-ОПК-1, 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

* – 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	22	0
1-8	**Раздел 1 Концепция и теоретические основы безопасности критической информационной инфраструктуры**	4	12	
1 - 2	**Тема 1. Концептуальные основы создания и применения системы защиты объектов и управления безопасностью информации в АСУ.** Эволюция и парадоксы нормативной базы объектов КИИ. Цели, задачи и этапы создания и применения системы защиты. Анализ уязвимости объектов и рисков потери ресурсов. Модели угроз. Модели нарушителей. Выявление и оценка основных видов угроз ИБ. Управление ИБ в АСУ. Задачи УИБ. Модель технологического цикла управления средствами обеспечения безопасностью информации (БИ). Формирование интегральной модели обеспечения ИБ в неоднородных АСУ. Протоколы управления ключевой и парольной защитой.	Всего аудиторных часов		
		1	2	
		Онлайн		

3 - 4	**Тема 2. Положения концепции защиты и защита объектов критической информационной инфраструктуры.** Основные положения концепции защиты объектов (ЗО) критической информационной инфраструктуры (КИИ). Основные положения Федерального Закона от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктурой РФ». Категорирование объектов по степени угроз. Анализ рисков. Модели оценки ценности развединформации. Общие принципы и состав систем обеспечения безопасности значимого объекта (организации, предприятия). Методика определения критических процессов на объектах КИИ. Принципы защиты и построения защиты значимых объектов КИИ.	Всего аудиторных часов		
		1	4	
		Онлайн		
5 - 6	**Тема 3. Модель угроз и технические каналы утечки информации. Безопасность информации, обрабатываемой на объектах КИИ. Общая характеристика технической разведки (ТР). Основы противодействия техническим** Общие принципы формирования модели угроз информационной безопасности (УИБ). Выявление и анализ угроз информационной безопасности. Формирование и анализ модели нарушителя. Цели и задачи технической разведки. Принцип организации и ведение технической разведки. Классификация технической разведки. Демаскирующие признаки. Физические основы технических средств разведки. Основы противодействия техническим средствам разведки. Основные направления противодействия техническим средствам разведки.	Всего аудиторных часов		
		1	2	
		Онлайн		
7 - 8	**Тема 4. Участники обеспечения информационной безопасности Российской Федерации и их задачи. Системный подход в защите значимых объектов критической информационной инфраструктуры** Основные участники обеспечения информационной безопасности Российской Федерации и их задачи. ФСБ России. ФСТЭК России. ГосСОПКА. Роскомнадзор. Минкомсвязь России. Россвязь. Субъекты КИИ (РФ). Нормативные документы по КИИ. Основные положения системного подхода к защите значимых объектов КИИ. Цели, задачи и ресурсы системы защиты информации. Угрозы ИБ и меры по их предотвращению. Определение угроз безопасности объектов КИИ.Обеспечение безопасности значимых объектов критической информационной инфраструктуры.	Всего аудиторных часов		
		1	4	
		Онлайн		
9-15	**Раздел 2 Системы безопасности значимых объектов критической информационной инфраструктуры**	4	10	
9 - 10	**Тема 5. Категорирование объектов КИИ. Системы безопасности значимых объектов (субъектов КИИ). Стадии (этапы) работ по созданию систем безопасности** Оценка масштаба (возможных) последствий нарушения деятельности объекта критической информационной инфраструктуры. Определение категории значимости	Всего аудиторных часов		
		1	2	
		Онлайн		

	объекта КИИ. Порядок подготовки и отправки документов во ФСТЭК России на присвоение категории значимости объекту КИИ. Проектирование системы безопасности значимых объектов (субъектов КИИ). Стадии (этапы) работ по созданию систем безопасности. Сопровождение объектов КИИ в проверках ФСБ России и ФСТЭК России.			
11 - 12	**Тема 6. Комплексная политика защиты информации. Организация технической защиты информации и защиты значимых объектов КИИ** Политика комплексной защиты информации. Функции защиты информации. Задачи защиты информации. Средства и методы защиты информации. Система защиты информации (СЗИ). Расширение постановки задачи защиты. Задачи и структура государственной системы технической защиты информации и защиты ЗОКИИ. Структура построения и основные ТТх автоматизированных систем охраны стационарных удаленных объектов повышенной защищённости. Организация защиты ТЗКИ и ЗОКИИ. Основные организационные и технические меры по обеспечению безопасности ЗОКИИ и ТЗКИ.	Всего аудиторных часов		
		1	4	
		Онлайн		
13 - 14	**Тема 7. Требования по обеспечению безопасности объектов. Варианты подключения значимого объекта КИИ к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (Го** Анализ существующих нормативно-методических документов. Порядок определения степени конфиденциальности при обеспечении ИБ. Обоснование требуемого класса защищенности локальной вычислительной сети (ЛВС). Требования к классу и показателям защищенности ЛВС и СВТ. Варианты подключения ЗОКИИ к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).	Всего аудиторных часов		
		1	2	
		Онлайн		
15	**Тема 8. Взаимодействие значимого объекта субъекта критической информационной инфраструктуры с ГосСОПКА. Технический контроль ЗИ** Взаимодействие значимого объекта субъекта КИИ с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Технический контроль защиты объектов от утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Технический контроль значимых объектов от УИ за счет ВЧН, ВЧО и ВЧП. Технический контроль значимых объектов от утечки информации за счет АЭП. Технический контроль эффективности системы активного электромагнитного зашумления. Технический контроль звукоизоляции защищаемых помещений. Технический контроль противодействия техническим средствам (коммерческой) разведки.	Всего аудиторных часов		
		1	2	
		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 СЕМИНАРОВ

Недели	**Темы занятий / Содержание**
	4 Семестр
1 - 2	**Тема №1, 2** ПЗ №1. Концептуальные основы создания и применения системы защиты объектов. ПЗ №2. Концептуальные основы управления безопасностью информации в АСУ.
3 - 4	**Тема №3, 4** ПЗ №3. Основы создания и применения системы защиты объектов. ПЗ №4. Положения концепции защиты объектов критической информационной инфраструктуры и технической защиты информации.
5 - 6	**Тема №5, 6** ПЗ №5. Модель угроз и технические каналы утечки информации. Безопасность информации, обрабатываемой на объектах КИИ. ПЗ №6. Общая характеристика технической разведки (ТР). Основы противодействия средствам (коммерческой) разведки (ПДТР).
7 - 8	**Тема №7, 8** ПЗ №7. Участники обеспечения информационной безопасности Российской Федерации и их задачи. ПЗ №8. Системный подход к защите значимых объектов критической информационной инфраструктуры (КИИ).
9 - 10	**Тема №9, 10** ПЗ №9. Категорирование объектов критической информационной инфраструктуры. ПЗ №10. Системы безопасности значимых объектов (субъектов КИИ). Стадии (этапы) работ по созданию систем безопасности.
11 - 12	**Тема №11, 12** ПЗ №11. Комплексная политика защиты информации. ПЗ №12. Организация технической защиты информации и защиты значимых объектов КИИ.

13 - 14	**Тема №13, 14** ПЗ №13. Требования по обеспечению безопасности объектов. ПЗ №14. Варианты подключения значимого объекта КИИ к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).
15	**Тема №15, 16** ПЗ №15. Взаимодействие значимого объекта субъекта КИИ с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак. ПЗ №16. Технический контроль защиты информации.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, ГК Росатом, 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 атомной энергетике, обеспечение требованиям кибербезопасности и безопасности ЗОКИИ. 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.

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)**
ОПК-1	З-ОПК-1	З, КИ-8, КИ-15
	У-ОПК-1	З, КИ-8, КИ-15
	В-ОПК-1	З, КИ-15
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

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:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>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.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">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.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно»</td></tr>
</table>

			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 Р 15 Базы данных: основы, проектирование, разработка информационных систем, проекты. Курс лекций : учеб. пособие, Москва: НИЯУ МИФИ, 2020

2. 004 М 21 Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. : учеб. пособие для вузов., Москва: Горячая линия -Телеком, 2018

3. ЭИ Л 14 Сертификация информационных систем : учебное пособие, Санкт-Петербург: Лань, 2020

4. ЭИ Т 18 Современные операционные системы. 4-е изд. — (Серия «Классика computer science») : , Санкт-Петербург: Питер, 2021

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 – «Обеспечение значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники. В том числе в области аттестации объектов информатизации по требованиям безопасности информации; 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.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации (ЗОКИИ), 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 построения систем безопасности ЗОКИИ. 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.

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 внимания 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 зачёт или экзамен.

2. Лабораторные работы. Лабораторные работы не предусмотрены.

3. Практическая работа. На практическую работу выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических работ по отработке навыков предусматривает решение различного рода задач. Результаты, полученные в ходе выполнения практических работ, могут использоваться студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), контрольные работы, собеседование, методы обычного тестирования или тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами полученными в хоте выполнения практических работ.

Темы занятий

Раздел 1. Концепция и теоретические основы безопасности критической информационной инфраструктуры

Тема 1. Концептуальные основы создания и применения системы защиты объектов и управления безопасностью информации в АСУ

Эволюция и парадоксы нормативной базы объектов КИИ. Цели, задачи и этапы создания и применения системы защиты. Анализ уязвимости объектов и рисков потери ресурсов. Модели угроз. Модели нарушителей. Выявление и оценка основных видов угроз ИБ. Управление ИБ в АСУ. Задачи УИБ. Модель технологического цикла управления средствами обеспечения безопасностью информации (БИ). Формирование интегральной модели обеспечения ИБ в неоднородных АСУ. Протоколы управления ключевой и парольной защитой.

Тема 2. Положения концепции защиты и защита объектов критической информационной инфраструктуры

Основные положения концепции защиты объектов (ЗО) критической информационной инфраструктуры (КИИ). Основные положения Федерального Закона от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктурой РФ». Категорирование объектов по степени угроз. Анализ рисков. Модели оценки ценности развединформации. Общие принципы и состав систем обеспечения безопасности значимого объекта (организации, предприятия). Методика определения критических процессов на объектах КИИ. Принципы защиты и построения защиты значимых объектов КИИ.

Тема 3. Модель угроз и технические каналы утечки информации. Безопасность информации, обрабатываемой на объектах КИИ. Общая характеристика технической разведки (ТР). Основы противодействия техническим средствам (коммерческой) разведки

Общие принципы формирования модели угроз информационной безопасности (УИБ). Выявление и анализ угроз информационной безопасности. Формирование и анализ модели нарушителя. Цели и задачи технической разведки. Принцип организации и ведение технической разведки. Классификация технической разведки. Демаскирующие признаки. Физические основы технических средств разведки. Основы противодействия техническим средствам разведки. Основные направления противодействия техническим средствам разведки.

Тема 4. Участники обеспечения информационной безопасности Российской Федерации и их задачи. Системный подход в защите значимых объектов критической информационной инфраструктуры

Основные участники обеспечения информационной безопасности Российской Федерации и их задачи. ФСБ России. ФСТЭК России. ГосСОПКА. Роскомнадзор. Минкомсвязь России. Россвязь. Субъекты КИИ (РФ). Нормативные документы по КИИ. Основные положения системного подхода к защите значимых объектов КИИ. Цели, задачи и ресурсы системы защиты информации. Угрозы ИБ и меры по их предотвращению. Определение угроз безопасности объектов КИИ.Обеспечение безопасности значимых объектов критической информационной инфраструктуры.

Раздел 2. Системы безопасности значимых объектов критической информационной инфраструктуры

Тема 5. Категорирование объектов КИИ. Системы безопасности значимых объектов (субъектов КИИ). Стадии (этапы) работ по созданию систем безопасности

Оценка масштаба (возможных) последствий нарушения деятельности объекта критической информационной инфраструктуры. Определение категории значимости объекта КИИ. Порядок подготовки и отправки документов во ФСТЭК России на присвоение категории значимости объекту КИИ. Проектирование системы безопасности значимых объектов (субъектов КИИ). Стадии (этапы) работ по созданию систем безопасности. Сопровождение объектов КИИ в проверках ФСБ России и ФСТЭК России.

Тема 6. Комплексная политика защиты информации. Организация технической защиты информации и защиты значимых объектов КИИ

Политика комплексной защиты информации. Функции защиты информации. Задачи защиты информации. Средства и методы защиты информации. Система защиты информации (СЗИ). Расширение постановки задачи защиты. Задачи и структура государственной системы технической защиты информации и защиты ЗОКИИ. Структура построения и основные ТТх автоматизированных систем охраны стационарных удаленных объектов повышенной защищённости. Организация защиты ТЗКИ и ЗОКИИ. Основные организационные и технические меры по обеспечению безопасности ЗОКИИ и ТЗКИ.

Тема 7. Требования по обеспечению безопасности объектов. Варианты подключения значимого объекта КИИ к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА)

Анализ существующих нормативно-методических документов. Порядок определения степени конфиденциальности при обеспечении ИБ. Обоснование требуемого класса защищенности локальной вычислительной сети (ЛВС). Требования к классу и показателям защищенности ЛВС и СВТ. Варианты подключения ЗОКИИ к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Тема 8. Взаимодействие значимого объекта субъекта критической информационной инфраструктуры с ГосСОПКА. Технический контроль ЗИ

Взаимодействие значимого объекта субъекта КИИ с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Технический контроль защиты объектов от утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Технический контроль значимых объектов от УИ за счет ВЧН, ВЧО и ВЧП. Технический контроль значимых объектов от утечки информации за счет АЭП. Технический контроль эффективности системы активного электромагнитного зашумления. Технический контроль звукоизоляции защищаемых

помещений. Технический контроль противодействия техническим средствам (коммерческой) разведки.

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 значимых объектов критической информационной инфраструктуры», место курса в различных областях науки и техники. В том числе в области аттестации объектов информатизации по требованиям безопасности информации; 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.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации (ЗОКИИ), 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 построения систем безопасности ЗОКИИ. 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.

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 внимания 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 зачёт или экзамен.

2. Лабораторные работы

Лабораторные работы не предусмотрены.

3. Практическая работа

На практическую работу выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических работ по отработке навыков предусматривает решение различного рода задач. Результаты, полученные в ходе выполнения практических 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), контрольные работы, собеседование, методы обычного тестирования или тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами полученными в хоте выполнения практических работ.

4. 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):

Гавдан Григорий Петрович

Рецензент(ы):

Дураковский А.П.