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 КИБЕРБЕЗОПАСНОСТИ АТОМНОЙ ЭНЕРГЕТИКИ

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
1	3	108	32	0	0		76	0	З
Итого	3	108	32	0	0	0	76	0	

АННОТАЦИЯ

Целью учебной дисциплины «Основы кибербезопасности атомной энергетики» является формирование основополагающих знаний по текущим и перспективным вопросам обеспечения кибербезопасности в атомной отрасли при неукоснительном выполнении требований ядерной безопасности и с учетом возрастающей роли России в мировой атомной энергетике.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины являются обеспечение требуемого уровня знаний, умений и навыков у студентов для обеспечения кибербезопасности в атомной отрасли при неукоснительном выполнении требований ядерной безопасности и с учетом возрастающей роли России в мировой атомной энергетике.

Задачами дисциплины являются освоение следующих основных тем:

работа энергетических систем и роль в них ядерно-энергетических установок (ЯЭУ),

ядерно-физические процессы в ядерном реакторе, основные режимы его работы;

наиболее распространенные типы реакторов, ядерно-топливный цикл;

основные положения ядерной безопасности;

МАГАТЭ и международная шкала ядерных событий;

от защиты информации до кибербезопасности;

задачи и проблемы кибербезопасности в ядерной энергетике;

история и структура атомной отрасли России.

Дисциплина «Основы кибербезопасности атомной энергетики» 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 кибербезопасности атомной энергетики» 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 и умениями основ информационной безопасности.

Знания, полученные при изучении дисциплины «Основы кибербезопасности атомной энергетики» 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 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ иди информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; в автоматизированных системах; технические средства контроля эффективности мер защиты информации; современные информационные

			технологии (операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; средства контроля защищенности информации от несанкционированного доступа. ; У-ПК-2[1] - Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее. ; В-ПК-2[1] - Владеть: основами выполнения анализа защищенности компьютерных систем с использованием сканеров безопасности; основами

			составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами испытаний программно-технического средств защиты информации от несанкционированного доступа и специальных воздействий на нее.
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	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;

		Основание: Профессиональный стандарт: 06.030, 06.032	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	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

		стандарт: 06.033, 06.034	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.

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
	1 Семестр						
1	Принципы работы и устройства ядерных энергетических установок	1-8	16/0/0		25	КИ-8	З-ПК-2, У-ПК-2, З-ПК-2.1, У-ПК-2.1, З-ПК-2.2, У-ПК-2.2, З-ПК-2.3, У-ПК-

							2.3
2	Кибербезопасность, ядерная и информационная безопасность объектов ядерной энергетики	9-16	16/0/0		25	КИ-16	З-ПК-2, У-ПК-2, В-ПК-2, 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
	Итого за 1 Семестр		32/0/0		50		
	Контрольные мероприятия за 1 Семестр				50	З	З-ПК-2, У-ПК-2, В-ПК-2, 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

* – 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.**
	1 Семестр	32	0	0
1-8	**Принципы работы и устройства ядерных энергетических установок**	16	0	0
1	**Тема 1. Энергетические системы и место атомной энергетики в них.** Особенности производства электроэнергии и ее потребления. Суточный, недельный и годовой циклы. Типы электростанций, их особенности и перспективы. Коэффициент использования установленной мощности. История возникновения и развития атомной энергетики. Роль атомной энергетики в мировом хозяйстве в настоящее время и в перспективе. География атомной энергетики.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
2	**Тема 2. Ядерно-физические процессы в атомном реакторе.** Состав атомного ядра. Взаимодействие нейтронов с веществом. Типы ядерных нейтронных реакций. Радиоактивность. Деление ядер. Энергия деления. Осколки деления, их распределение. Запаздывающие нейтроны. Изменения изотопного состава ядерного топлива. Накопление продуктов деления. Цепная реакция деления. Энерговыделение. Коэффициент размножения нейтронов.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
3	**Тема 3. Ядерное топливо и ядерный топливный цикл.** Ядерное горючее. Особенности урана и его распространение в природе. Обогащение урана, способы технической реализации. Технологическая цепочка	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0

	движения. Замкнутый топливный цикл, его основные характеристики. Воспроизводство ядерного горючего, его техническая реализуемость. Характеристики процесса воспроизводства. Проблемы захоронения ядерных отходов.			
4 - 5	**Тема 4. Математические модели физических процессов в ядерном реакторе.** Особенности математического описания цепной реакции деления. Схема баланса нейтронов в ядерном реакторе. Точечная модель, основные допущения при ее применении. Основные математические соотношения. Линеаризация уравнений кинетики. Передаточная функция реактора, ее особенности для критического, подкритического и надкритического реактора.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
6 - 7	**Тема 5. Ядерный реактор как объект управления.** Общая схема ядерной энергетической установки (ЯУЭ), включая ее тепловую часть. Физические процессы в ЯУЭ, их взаимосвязь. Классификация ядерных реакторов по назначению. Типовая конструкция ядерного реактора. Теплоносители и замедлители, их основные характеристики. Способы управления цепной реакцией. Реактивность, ее единицы. Органы управления ядерным реактором. Конструкции и технические характеристики стержней управления. Движение топлива на АЭС, Конструктивные особенности различных типов реакторов.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
8	**Тема 5. Основные режимы работы реактора.** Минимально контролируемый уровень мощности реактора. Тепловая и электрическая мощность. Физический и энергетический пуски реактора. Работа на энергетических уровнях мощности. Переход с одного уровня мощности реактора на другой. Останов, плановый и аварийный. Особенности управления реактором на различных режимах работы. Общая схема управления мощностью реактора.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
9-16	**Кибербезопасность, ядерная и информационная безопасность объектов ядерной энергетики**	16	0	0
9	**Тема 6. Строительство АЭС.** Выбор места строительства АЭС. Блочный принцип сооружения атомных энергетических объектов. Характер помещений на АЭС, условия труда эксплуатационного персонала. БЩУ и ЦЩУ. География действующих, строящихся и проектируемых АЭС в России и за рубежом.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
10	**Тема 7. Безопасность ядерного реактора.** Обеспечение безопасности на различных этапах основной цепочки технологического процесса в реакторе. Типы аварий. Активная и пассивная защита. Концепция внутренней безопасности. Система управления защитой (СУЗ). Особенности СУЗ для различных типов реакторов. Правила ядерной безопасности.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
11	**Тема 8. Международная шкала ядерных событий.** Сфера применения единой шкалы. Основы классификации событий. Содержание шкалы. Примеры прошлых ядерных событий. Особенности и причины аварий на Чернобыльской АЭС и в Фукусиме. Влияние крупных	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0

	аварий на концепцию безопасности.			
12	**Тема 8. Источники информации на ядерном объекте – измерения и результаты экспериментов.** Измерительные системы на ядерном реакторе, прямые и косвенные измерения, их особенности. Ядерно-физический контроль. Измерение реактивности. Измерение распределения энерговыделения. Эксперименты во время физического и энергетического пусков, при работе на энергетических уровнях мощности. Построение пусковой кривой.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
13	**Тема 9. Особенности реакторов на быстрых нейтронах.** Проблема воспроизводства ядерного горючего. Ядерно-физические и конструктивные особенности реакторов на быстрых нейтронах. Технические характеристики реакторов типа БН, особенности их управления, перспективы развития. Реактор типа БРЕСТ, программа «Прорыв».	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
14	**Тема 10. Автоматизированные системы объектов атомной энергетики.** Информационные потоки на АЭС. Классы и типы используемых программ. Роль автоматизированной системы в обеспечении ядерной безопасности.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
15	**Тема 11. Атомная отрасль России.** История ее возникновения и развития. Роль МИФИ в становлении и развитии отрасли Задачи, решаемые Росатомом. Его структура. Тенденции развития. Взаимодействие Росатома с МАГАТЭ. Стабилизирующая роль современной атомной энергетики в геополитике.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
16	**Тема 12. Кибербезопасность.** Определение. Проблема терминологии в области кибербезопасности. Киберпространство, его составные части. Киберугрозы. Состояние кибербезопасности в атомной энергетике. Субъекты киберсреды. Направления исследований по кибербезопасности. Концепция кибербезопасности АЭС. Основные типы угроз для АСУ ТП, Методы обеспечения кибербезопасности в жизненном цикле АСУ ТП АЭС. Проблема импортозамещения.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0

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

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов. Последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания. Поисковые методы; постановка познавательных задач. В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы 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 и обеспечение требованиям кибербезопасности. 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)**
ПК-2	З-ПК-2	З, КИ-8, КИ-16
	У-ПК-2	З, КИ-8, КИ-16
	В-ПК-2	З, КИ-16
ПК-2.1	З-ПК-2.1	З, КИ-8, КИ-16
	В-ПК-2.1	З, КИ-16
	У-ПК-2.1	З, КИ-8, КИ-16
ПК-2.2	У-ПК-2.2	З, КИ-8, КИ-16
	З-ПК-2.2	З, КИ-8, КИ-16
	В-ПК-2.2	З, КИ-16
ПК-2.3	З-ПК-2.3	З, КИ-8, КИ-16
	У-ПК-2.3	З, КИ-8, КИ-16
	В-ПК-2.3	З, КИ-16

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» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.</td></tr>
</table>

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Н35 Аннотации докладов Т.1 Фундаментальные исследования и физика частиц. Атомная энергетика и ядерные технологии. Ядерные системы и материалы. Физика неравновесных атомных систем и композитов, Москва: НИЯУ МИФИ, 2015

2. ЭИ Д 46 Кибербезопасность. стратегия атак и обороны : , Москва: ДМК Пресс, 2020

3. ЭИ В75 Мировая экономика и особенности мирового атомного рынка : методические рекомендации к изучению курса, Москва: НИЯУ МИФИ, 2015

4. ЭИ К60 Ионизирующая радиация: воздействие, риски, общественное восприятие : , А. Б. Колдобский, Москва: МИФИ, 2008

5. 539.1 К49 Основы ядерной и нейтронной физики : учеб. пособие, А.Н. Климов, Москва: МИФИ, 2004

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 621.039 О-75 Основы безопасного обращения и обезвреживания радиоактивных отходов : Учебное пособие, Москва: НИЯУ МИФИ, 2019

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 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.

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.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ГК Росатом и 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 основам кибербезопасности атомной энергетики. 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.

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.

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.

Особенности изучения разделов дисциплины

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ГК Росатом и 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 основам кибербезопасности атомной энергетики. 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.

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).

Допускается варьирование в программе дисциплины набора, последовательности и объема в часах разделов лекционного курса и практических работ. При организации изучения дисциплины рекомендуется в лекционном курсе освещать только проблемные вопросы, оставляя более подробный анализ содержания дисциплины на практические занятия, а также для самостоятельной проработки, в том числе при подготовке к текущему и итоговому контролю знаний.

Автор(ы):

Иваненко Виталий Григорьевич, д.т.н., профессор

Рецензент(ы):

Дураковский А.П.