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 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

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	8	24	0		40	0	Э
Итого	3	108	8	24	0	4	40	0	

АННОТАЦИЯ

Дисциплина «Основы информационной безопасности критически важных объектов» имеет целью обучить студентов (слушателей) основным принципам построения и технологиям, используемых в настоящее время при создании подсистем обеспечения безопасности ключевых систем информационной инфраструктуры и рекомендованных международными организациями по стандартизации в области ИБ и российскими нормативными актами и стандартами. Курс позволяет дать понятие студентам основные представления об основах обеспечения безопасности ключевых систем информационной инфраструктуры.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В настоящее время созданы и активно внедряются технологии передачи данных на основе пакетных коммуникаций. Развитие таких технологий, создание сети Интернет на основе стека протоколов TCP/IP, их активное внедрение во все сферы человеческой деятельности, обострило проблему информационной безопасности ресурсов, которые поддерживаются с помощью коммуникационных технологий и существенно усложнило её разрешении. В связи с отмеченным обстоятельством особую важность приобретают вопросы защиты от деструктивных информационных воздействий больших и сложно организованных, значимых с позиций национальной безопасности объектов. В мировой практике такие объекты принято именовать критически важными.

Целью настоящей дисциплины является обучение основным подходам к решению существующих на этом пути задач, с учетом объективно существующих сложностей.

Задачами дисциплины являются освоение следующих основных тем:

Содержание традиционной системы мер и действий, направленных на обеспечение безопасности объекта от деструктивных информационных воздействий, которое зависит от целого ряда обстоятельств (факторов). К их числу относятся: назначение; свойства объекта и его среды окружения; активы, подлежащие защите; угрозы, которым они могут быть подвержены, и возникающие при этом риски; отношение администрирующей объект организации к предоставлению (использованию) активов и цели обеспечения их безопасности.

В результате изучения, систематизации и формализации перечисленных факторов формируются требования к средствам обеспечения безопасности подконтрольного объекта как основа для программы практических действий на этом направлении.

Дисциплина «Основы информационной безопасности критически важных объектов» 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 информационной безопасности критически важных объектов» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» (блок Б1.ДВ.1.2.1 РУП).

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 информационной безопасности критически важных объектов» 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	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.

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	Безопасность информационных технологий и защита критически важных объектов	1-8	4/12/0		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	Оценка уровня информационной безопасности критически важных объектов, методы и средства защиты	9-16	4/12/0		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		8/24/0		50		
	Контрольные мероприятия за 1 Семестр				50	Э	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
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	1 Семестр	8	24	0
1-8	**Безопасность информационных технологий и защита критически важных объектов**	4	12	0
1	**Тема 1. Введение. Основы государственной информационной политики и информационной безопасности Российской Федерации** Основные понятия, общеметодологические принципы обеспечения информационной безопасности. обеспечения информационной безопасности. Понятие сообщение. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере.	Всего аудиторных часов		
		1	2	0
		Онлайн		
		0	0	0
2 - 3	**Тема 2. Базовая терминология в сфере**	Всего аудиторных часов		

	информационной безопасности. Эволюция понятия «Информационная безопасность». Доктрина информационной безопасности Российской Федерации. Информационная безопасность объекта. Свойства информации. Критически важные объекты. Ключевая (критически важная) система информационной инфраструктуры.	1	2	0
		Онлайн		
		0	0	0
4 - 5	**Тема 3. Нормативно-правовое обеспечение.** Предмет и содержание проблемы. Нормативно правовая база ИБ в РФ. Структура законодательства РФ. Техническое регулирование в области ИБ. Стандартизация обеспечения ИБ. Нормативно-правовое обеспечение безопасности КВО.	Всего аудиторных часов		
		1	2	0
		Онлайн		
		0	0	0
6 - 7	**Тема 4. Исходная концептуальная схема обеспечения ИБ. Деструктивные воздействия на передаваемую информацию (сообщение).** Проблемы информационной безопасности в сфере государственного и муниципального управления. Проблема обеспечения безопасности информации, технологий её обработки, средств и систем, как их носителей. Виды деструктивных воздействий при передаче информации в виде сведений, связанных с её предварительным преобразованием в сообщение, которое отчуждается от её источника. Технологии передачи данных на основе пакетных коммуникаций. Создание метасети Интернет на основе стека протоколов TCP/IP, её активное внедрение во все сферы человеческой деятельности. Информационные процессы в сфере государственного и муниципального управления. Виды информации и информационных ресурсов в сфере ГМУ. Состояние и перспективы информатизации государственной сферы.	Всего аудиторных часов		
		1	2	0
		Онлайн		
		0	0	0
7	**Тема 5. Защита информации от несанкционированного доступа (ЗИ от НСД)** Введение. Основные модели защиты. Авторизация субъектов доступа. Основные способы НСД. Основы ЗИ от НСД. Категорирование информации. Управление доступом в АС. Обзор программно-аппаратных средств ЗИ от НСД.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
8	**Тема 6. Компьютерные вирусы. Защита информации от воздействий вредоносных программ.** Понятие и основные типы компьютерных вирусов. Файловые вирусы; Загрузочные вирусы; Комбинированные вирусы; Программные вирусы; Макровирусы; «Троянские» программы; Полиморфные вирусы; Стелс – вирусы. Пути проникновения вирусов в ПК и механизм распределения вирусных программ. Признаки появления вирусов.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
9-16	**Оценка уровня информационной безопасности критически важных объектов, методы и средства защиты**	4	12	0
9 - 11	**Тема 7. Криптографические методы защиты информации** Общесистемные аспекты криптологии. Основные задачи,	Всего аудиторных часов		
		1	4	0
		Онлайн		

	составляющие предмет теории защиты информации, и криптографические методы решения первой и второй задач, которые реализуются соответствующими криптосистемами как при хранении, так и при передаче информации: 1) обеспечение надежного хранения сообщений и управление доступом к информации со стороны различных категорий пользователей, в том числе, блокирование доступа к информации со стороны нарушителя (защита от НСД); 2) при передаче информации между законными пользователями обеспечение надежной защиты от искажения сообщений и от ознакомления с ними посторонних лиц или нарушителя. Основные понятия криптологии. Криптографические алгоритмы. Криптографические протоколы. Ключевая подсистема криптосистемы.	0	0	0
12 - 13	**Тема 8. Защита информации от утечки по техническим каналам.** Технические каналы утечки: Визуально-оптические каналы. Акустические каналы. Электромагнитные каналы. Материально-вещественные каналы. Радиоэлектронные каналы утечки информации. Положение об организации ИБ при хранении, обработке и передаче по каналам связи информации. Этапы организации мероприятий по защите утечки техническим каналам информации на защищаемом объекте: Подготовительный, предпроектный. Проектирование СТЗИ. Этап ввода в эксплуатацию защищаемого объекта и системы технической защиты информации. Основные меры защиты информации от утечки по техническим каналам. Организационные меры защиты: временные ограничения, территориальные ограничения. Способы и средства ТКЗИ от утечки по техническим каналам утечки.	Всего аудиторных часов 1	4	0
		Онлайн 0	0	0
14 - 15	**Тема 9. ИБ автоматизированных систем критически важных объектов.** Введение. Критически важные объекты. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Автоматизированная система управления производственными и технологическими процессами КВО инфраструктуры РФ - комплекс аппаратных и программных средств, информационных систем и информационно- телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса КВО, нарушение (или прекращение) функционирования которых	Всего аудиторных часов 1	2	0
		Онлайн 0	0	0

	может нанести вред внешнеполитическим интересам РФ, стать причиной аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизации работы учреждений, предприятий или организаций, нанесения материального ущерба в крупном размере, смерти или нанесения тяжкого вреда здоровью хотя бы одного человека и (или) иных тяжелых последствий. Структура АСУ ТП. Автоматизированная система управления технологическим процессом (АСУ ТП) КВО— комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на КВО. АСУ ТП характеризуются обеспечением комплексной автоматизацией технологических операций на всем производстве или отдельном участке КВО. АСУ ТП представляет собой программно-аппаратный комплекс, состоящий из: * автоматизированных рабочих мест (станция оператора, станция инженера, станция инженера КИП); * программируемого логического контроллера (ПЛК); * контрольно-измерительных приборов и автоматики (КИП). Обеспечение ИБ в АСУТП. Объекты защиты в АСУ ТП. Угрозы ИБ для АСУ ТП. Система обеспечения ИБ АСУ ТП. Аттестация АСУТП.			
16	**Тема 10. ИБ и системы физической защиты критически важных объектов** Введение. СФЗ как поддерживающая система обеспечения безопасности информации на объекте. СФЗ как поддерживающая система обеспечения безопасности информации на объекте. ГОСТ Р ИСО/МЭК 27002-2012 «ИТ. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента ИБ»: 9 Физическая безопасность и защита от воздействий окружающей среды Зоны безопасности. Цель: предотвращать неавторизованный физический доступ, повреждение и воздействие в отношении помещений и информации организации. Средства обработки критической или чувствительной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами, контролирующими вход. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия. Уровень защищенности должен быть соразмерен выявленным рискам. Обеспечение безопасности информации в самой СФЗ. Реализация подсистем ФЗ: Средства вычислительной техники; Микропроцессорные устройства; Средства телекоммуникации; Средства связи; Средства управления; Средства отображения; Средства документирования;	Всего аудиторных часов		
		1	2	0
		Онлайн		
		0	0	0

	Средства обработки, хранения и отображения видеоинформации; Средства управления доступом. Функционирование СФЗ: обязательное участие человека. Обеспечение ИБ СФЗ ядерных объектов. Обеспечение ИБ систем учета и контроля ядерных материалов. Обеспечение ИБ при использовании систем связи на ядерных объектах. Постановления Правительства РФ от 14.03.2014 N 191 «Об утверждении Правил физической защиты ядерных материалов; ядерных установок и пунктов хранения ядерных материалов» (в ред. Постановлений Правительства РФ от 22.04.2009 N 351; от 08.010.2010 N 702, от 04.02.2011 N 48, от 16.05.2011 N 364, от 28.08.2012 N 863, от 16.02.2013 N 127, от 18.02.2014 N 125, от 14.03.2014 N 191): I. Общие положения II. Государственная система физической защиты III. Организация и осуществление физической защиты на ядерном объекте IV. Основные требования к организации физической защиты ядерных материалов, ядерных установок при перевозке и транспортировании V. Государственный надзор, ведомственный и объектовый контроль за физической защитой VI. Уведомление о несанкционированных действиях Приложение 1: Категории ядерных материалов Приложение 2: Категории последствий несанкционированных действий в отношении предметов физической защиты Приложение 3: Требования к размещению предметов физической защиты на ядерном объекте			

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**
	1 Семестр
1 - 8	**Укажите название пункта** Механизмы обеспечения национальных интересов российской федерации в информационной сфере

	Уровни обеспечения информационной безопасности Национальные интересы в информационной сфере Источники и содержание угроз в информационной сфере Задачи внутренней и внешней политики государства по обеспечению информационной безопасности. Анализ мировых лидеров микроэлектронной и компьютерной промышленности Инфраструктура единого информационного пространства Российской Федерации Способы и методы повышения эффективности использования государственных информационных ресурсов отечественной индустрии информационных услуг Анализ развития производств в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи Основные отечественные фундаментальные и прикладные исследования, разработки в сферах информатизации, телекоммуникации и связи
9 - 16	**Укажите название пункта** Анализ конкурентоспособных российских информационных технологий; Цель, задачи концепций информационных войн. Средства противоборства. Анализ состояния информационной безопасности Российской Федерации Государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок Нормативные документы в области информационной безопасности Структура, функции и задачи органа, обеспечивающего информационную безопасность (ФСТЭК России) Структура, функции и задачи органа, обеспечивающего информационную безопасность (Роскомнадзор). Структура, функции и задачи органа, обеспечивающего информационную безопасность. (Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации) Структура, функции и задачи органа, обеспечивающего информационную безопасность (Комитет Государственной думы по безопасности) Политика информационной безопасности и защиты информационной системы государства

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. Лекции и практические занятия проводятся с использованием ППП «MS Office» (Power Point) и отображением на экране материалов занятий.

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	Э, КИ-8, КИ-16
	У-ПК-2	Э, КИ-8, КИ-16
	В-ПК-2	Э, КИ-16
ПК-2.1	З-ПК-2.1	Э, КИ-8, КИ-16
	В-ПК-2.1	Э, КИ-16
	У-ПК-2.1	Э, КИ-8, КИ-16
ПК-2.2	У-ПК-2.2	Э, КИ-8, КИ-16
	З-ПК-2.2	Э, КИ-8, КИ-16
	В-ПК-2.2	Э, КИ-16
ПК-2.3	З-ПК-2.3	Э, КИ-8, КИ-16
	У-ПК-2.3	Э, КИ-8, КИ-16
	В-ПК-2.3	Э, 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:

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
75-84		C	
70-74		D	

			существенных неточностей в ответе на вопрос.
65-69	3 – «*удовлетворительно*»	E	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			
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.

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 П 54 Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов, Москва: Юрайт, 2022

3. ЭИ Н 56 Основы информационной безопасности : учебное пособие, Санкт-Петербург: Лань, 2022

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

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 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 – 15. 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.

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 – 15. 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).

Автор(ы):

Резниченко Сергей Анатольевич

Рецензент(ы):

Дураковский А.П.