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 № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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
3	3	108	32	32	0		44	0	ЗО
Итого	3	108	32	32	0	0	44	0	

АННОТАЦИЯ

Цель дисциплины - обеспечение требуемого уровня знаний, умений и навыков у студентов об организационно-правовых нормах и методах обеспечения информационной безопасности и защиты информации.

Дисциплина «Организационно-правовое обеспечение информационной безопасности» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом (ФГОС3++), содействует формированию научного мировоззрения и системного мышления; посвящена изучению основ организационного и правового обеспечения информационной безопасности и защиты информации.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является формирование общих представлений о принципах организационно-правового обеспечения информационной безопасности, лежащих в основе применения организационных и правовых норм и методов защиты информации.

Учебная дисциплина «Организационно-правовое обеспечение информационной безопасности» относится к разделу общеобразовательных дисциплин, логически и содержательно-методически взаимосвязанной с такими дисциплинами как «Управление информационной безопасностью». Именно глубокое изучение основ правоведения, организационного и правового обеспечения информационной безопасности должно сформировать устойчивые навыки использование законодательства, задающего нормативно-правовую базу, являющуюся необходимым элементом управленческой деятельности и организационно-правового обеспечения информационной безопасности.

Задачи дисциплины - это определение места организационного и правового обеспечения в системе безопасности предприятия (организации); установление организационных, нормативных и правовых основ и принципов защиты информации; разрешение общих и специфических вопросов организационного и правового обеспечения; раскрытие принципов, методов организационного и правового обеспечения информационной безопасности и защиты информации.

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».

Для усвоения учебной дисциплины «Организационно-правовое обеспечение информационной безопасности» студенты должны знать следующие дисциплины: "Правовые основы", «Информатика»; «Теория информации»; «Основы информационной безопасности» и др.

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**
организационно-управленческий			
Организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ; Разработка проектов организационно-распорядительных документов в области обеспечения безопасности значимых объектов критической информационной инфраструктуры	Контроль защищенности информации на объектах информатизации	ПК-8 [1] - Способен использовать навыки составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области ИБ или в области информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.033, 06.034	З-ПК-8[1] - Знать: профессиональная и криптографическая терминология в области безопасности информации; эталонная модель взаимодействия открытых систем, основные протоколы, последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетей; принципы работы элементов и функциональных узлов электронной аппаратуры, типовые схемотехнические решения основных узлов и блоков электронной аппаратуры; принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспечения. организационно-распорядительная документация по защите информации на объекте информатизации; современные информационные технологии

			(операционные системы, базы данных, вычислительные сети); технические каналы утечки акустической речевой информации; методы защиты информации от утечки по техническим каналам; способы защиты акустической речевой информации от утечки по техническим каналам. ; У-ПК-8[1] - Уметь: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять перечень информации (сведений)ограниченного доступа, подлежащих защите в организации; определять условия расположения объектов информатизации относительно границ контролируемой зоны; разрабатывать аналитическое обоснование необходимости создания системы защиты информации в организации; разрабатывать разрешительную систему доступа к информационным ресурсам, программным и техническим средствам

			автоматизированных (информационных) систем организации. ; В-ПК-8[1] - Владеть: основами применения средств схемотехнического проектирования и современной измерительной аппаратуры; основами оптимизации работ электронных схем с учетом требований по защите информации; основами организации проведения научных исследований по вопросам технической защиты информации, выполняемых в организации.

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
	3 Семестр						
1	1. Организационная защита конфиденциальной информации	1-8	16/16/0		25	КИ-8	З-ПК-8, У-ПК-8, В-ПК-8
2	2. Правовая защита конфиденциальной информации	9-16	16/16/0		25	КИ-16	З-ПК-8, У-ПК-8, В-ПК-8
	Итого за 3 Семестр		32/32/0		50		
	Контрольные мероприятия за 3 Семестр				50	ЗО	З-ПК-8, У-ПК-8, В-ПК-8

* – 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
ЗО	Зачет с оценкой
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	3 Семестр	32	32	0
1-8	**1. Организационная защита конфиденциальной информации**	16	16	0
1	**Тема 1. Сущность организационной ЗКИ. Методы и формы организационной ЗКИ** Введение в курс «Организационная защита конфиденциальной информации». Предмет и задачи курса «Организационная защита конфиденциальной информации». Концептуальные основы информационной безопасности в Российской Федерации. Информационная безопасность в Российской Федерации. Способы, источники и методы промышленно-экономического шпионажа. Организационные, правовые основы защиты конфиденциальной информации (ЗКИ). Сущность организационной ЗКИ. Методологические основы организации системы ЗКИ. Назначение системы ЗКИ. Принципы построения системы ЗКИ. Стратегия и способы ЗКИ. Каналы утечки конфиденциальной и др. информации. Методы и формы организационной ЗКИ. Классификация организационных мероприятий по ЗКИ. Определение мер защиты.	Всего аудиторных часов 2 Онлайн 0	2 0	0 0
2	**Тема 2. Подбор персонала и оформление допуска для работы с конфиденциальной информацией. Обучение сотрудников правилам и приёмам работы** Подбор кандидатов. Изучение резюме и изучение кандидатов. Собеседование с экспертом. Рассматривается медицинская справка, при необходимости проведение тестирования и анкетирования кандидата. Принятие решения руководством на приём. Подписание обязательства о неразглашении тайны фирмы. Предупреждение об ответственности за разглашение конфиденциальной информации. Ознакомление с должностной инструкцией. Изучение личных, моральных и профессиональных качеств сотрудника в течение испытательного срока. Обучение правилам работы с конфиденциальной информацией и документами. Проводение инструктажей, проверка знаний. Анализ результатов работы сотрудника в течение испытательного срока. При оформлении допуска к конфиденциальной информации к сотрудникам выдвигают требования, соразмерные с важностью сведений. Обязательное требование - запрет на разглашение внутренней	Всего аудиторных часов 2 Онлайн 0	2 0	0 0

	информации. В зависимости от ценности защищаемых сведений могут выдвигаться и др. требования.			
3	**Тема 3. Лицензирование деятельности оргвнизаций для проведения работ, связанных с конфиденциальной информацией** Лицензирование деятельности по технической ЗКИ. Термины и определения по ЗКИ. Лицензируемая деятельность. Лицензируемый орган. Лицензируемый сбор. Лицензионные требования, предъявляемые: к соискателю лицензии на осуществление лицензируемого вида деятельности; к лицензиату при осуществлении лицензируемого вида деятельности. Лицензионные требования. Перечень документов, предоставляемых с целью получения лицензии. Получение лицензии.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
4	**Тема 4. Режим хранения носителей конфиденциальной информации. Организация физической охраны предприятия, пропускного и внутриобъектового режимов** Требования внутриобъектового режима в организации. Защита помещений. Классификация помещений в зависимости от условий доступа. Классификация охраняемых объектов. Носители конфиденциальной информации и их классификация. Виды и уровень угроз безопасности информации в защищаемом момещении. Порядок сдачи под охрану и приём из-под охраны защищаемых и иных помещений и др. Физическая охрана предприятия. Оперативный дежурный на предприятии. Руководитель подразделения личной охраны и его обязанности. Сотрудники подразделения и их обязанности. Система охраны. Методы, меры и способы ЗКИ обеспечивающие нормальную работу предприятия.Пропускной и внутриобъектовый режим предприятия. Оборудование пропускных пунктов и КПП. Допуск на предприятие. Организация внутриобъектового режима.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
5	**Тема 5. Организация защиты конфиденциальной информации при проведении закрытых мероприятий** Разглашение ЗКИ. Этапы проведения закрытых совещаний или переговоров. Плановые и внеплановые закрытые совещания или переговоры. Доступ к ним сотрудников организации. Приглашение сторонних лиц на закрытые совещания или переговоры. Ответственность за обеспечение ЗКИ и сохранение тайны организации на совещании. Подготовка закрытого совещания. Оформление списков и организация допуска сторонних лиц на закрытые совещания и переговоры. Рекламно-выстовочный материал.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
6	**Тема 6. Организация защиты конфиденциальной информации при осуществлении международного сотрудничества** Организация работы по обеспечению режима конфиденциальности в связи с предстоящим приёмом	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0

	иностранцев в данной организации. Разработка, согласование и утверждение программы приёма иностранцеводготовка. Подготовка плана мероприятий. Приём иностранцев. Подведение итогов выполнения запланированных режимных мероприятий. Определение персонального состава, привлекаемого к работе с иностранцами. Организация телефонных переговоров. Подготовка производственных помещений. Маршрут передвижения. Подготовка справок в службу безопасности, отражающих вопросы режимного характера.			
7	**Тема 7. Организация защиты конфиденциальной продукции в процессе транспортировки** Ответственность транспортников за сохранность перевозимых грузов. Краткий анализ положения дел на транспортных магистралях страны и криминогенная обстановка вокруг. Обеспечение надёжной защиты грузов. Определение маршрутов следования грузов. Численность личного состава охраны. Обеспечение контроля за прохождением груза и выполнение своих обязанностей охраной. Должностные инструкции. Особенности охраны грузов при использовании отдельных видов грузов. Охрана груза перевозимого в купе пассажирского поезда. Охрана груза перевозимого на автомобиле. Использование воздушного транспорта.	Всего аудиторных часов 2 Онлайн 0	2 0	0 0
8	**Тема 8. Организация служебного расследования по фактам утраты конфиденциальной информации** Разглашение сведений и утрата документов, содержащих КИ. Иные нарушения режима при работе с материалами КИ. Органицация служебного расследования. Назначение председателя и членов комиссии по проведению расследований связанных с нарушением режима и утраты документов КИ. Разработка должностых инструкций дляпредседателя и членов комиссии по проведению расследований связанных с нарушением режима и утраты документов КИ. Сроки проведения расследований и порядок их оформления. Отметка о всех фактах утраты КИ. Порядок оформления журнала учёта утраты КИ.	Всего аудиторных часов 2 Онлайн 0	2 0	0 0
9-16	**2. Правовая защита конфиденциальной информации**	16	16	0
9	**Тема 9. Теоретические основы информационной безопасности** Понятие, предмет и назначение учебной дисциплины «Правовые основы информационной безопасности». Информация как объект правового регулирования. Нормативно-правовые акты, регулирующие общественные отношения в сфере информационной безопасности. Понятие информационной безопасности. Национальные интересы в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Стратегические цели и основные направления обеспечения информационной безопасности. Понятие и структура информационной безопасности в Российской Федерации. Критическая инфраструктура Российской	Всего аудиторных часов 2 Онлайн 0	2 0	0 0

	Федерации.			
10	**Тема 10. Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации** Понятие, структура и виды общественных отношений в информационной сфере. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации. Конституционные права граждан в сфере информации. Право на доступ к информации. Общедоступная информация, информация ограниченного доступа. Государственная тайна. Персональные данные. Правовой статус государственных информационных систем. Информационные ресурсы.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
11	**Тема 11. Противодействие информационным угрозам** Понятие, признаки и исторические аспекты информационных войн. Информационная безопасность личности. Основы информационной гигиены личности. Проверка информации на достоверность. Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей. Субъекты и объекты правоотношений в области защиты от информации. Виды информации, распространение которой запрещено или ограничено. Стратегия противодействия экстремизму в Российской Федерации до 2025 года. Защита информации. Полномочия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Федеральный государственный контроль (надзор) за соблюдением требований в связи с распространением информации в информационно-телекоммуникационных сетях, в том числе сети "Интернет". Информация, причиняющая вред здоровью и (или) развитию детей. Информационная продукция для детей разного возраста (не достигших возраста шести лет; достигших возраста шести, двенадцати и шестнадцати лет). Контроль за деятельностью лиц, находящихся под иностранным влиянием.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
12	**Тема 12. Государственная политика Российской Федерации в области международной информационной безопасности** Государственная политика Российской Федерации в области международной информационной безопасности. Сущность международной информационной безопасности и основные угрозы международной информационной безопасности. Цель и задачи государственной политики Российской Федерации в области международной информационной безопасности. Основные направления реализации государственной политики в области международной информационной безопасности.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0

	Механизмы реализации государственной политики в области международной информационной безопасности. Международное законодательство в сфере информационной безопасности. Законодательство зарубежных стран, регулирующее правоотношения в сфере информационной безопасности.			
13	**Тема 13. Полномочия прокурора в сфере ограничения доступа к информации, распространяемой с нарушением закона и основные принципы организации информационной безопасности в органах прокуратуры** Порядок ограничения доступа к информации, распространяемой с нарушением закона. Полномочия органов прокуратуры Российской Федерации в сфере ограничения доступа к информации, распространяемой с нарушением закона. Полномочия органов прокуратуры Российской Федерации по противодействию экстремизму в информационной сфере. Информационная безопасность как один из базовых принципов цифровой трансформации органов прокуратуры Российской Федерации. Основные принципы организации информационной безопасности в органах прокуратуры Российской Федерации.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
14	**Тема 14. Защита интеллектуальных прав и ответственность за правонарушения в сфере информации** Законодательство Российской Федерации об интеллектуальной собственности. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права. Ответственность за правонарушения в информационной сфере. Общая характеристика и виды ответственности за правонарушения в информационной сфере. Уголовная ответственность в информационной сфере. Административная ответственность в информационной сфере. Дисциплинарная ответственность в информационной сфере. Материальная ответственность в информационной сфере.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
15	**Тема 15. Нормативное регулирование и ответственность субъектов КИИ** Требования ФЗ № 187 от 26.07.2017 «О безопасности критической информационной инфраструктуры (КИИ) Российской Федерации» (РФ) в отношении субъектов КИИ значительно претерпели изменения в Уголовном кодексе Российской Федерации (УК РФ). Федеральный закон (ФЗ) от 26.05.2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». Полномочия федеральных органов исполнительной власти в сфере обеспечения безопасности ЗО КИИ. Штрафы и установленные сроки давности привлечения к административной ответственности за нарушения в области обеспечения безопасности КИИ РФ. Признание правонарушений с длящимся сроком давности (с момента	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0

	обнаружения правонарушения проверяющим). Нормативные правовые акты (НПА) в области обеспечения безопасности значимых объектов (ЗО) КИИ и ИБ. Типы нарушений, статьи и наказания в области обеспечения безопасности значимых объектов (ЗО) КИИ и ИБ.			
16	**Тема 16. Актуальные проблемы правового и организационного обеспечения ИБ. Особенности организационно-правового обеспечения защиты информационных систем** Противодействие экстремистской деятельности в информационной сфере. Защита детей от информации, причиняющей вред их здоровью и развитию. Правовые проблемы обеспечения информационной безопасности в сети Интернет. Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении. Особенности организационно-правового обеспечения ЗКИ систем в сфере судопроизводства. Практика разработки и реализации политики ИБ корпоративных информационных систем. Понятие и виды юридической ответственности в области обеспечения ИБ. Субъекты и объекты правоотношений в области обеспечения ИБ. Преступность в информационной сфере как угроза ИБ при формировании информационного общества в условиях глобализации. Проблемы уголовно-правовой ответственности за информационные преступления. Проблемы международного сотрудничества и зарубежный опыт противодействия преступлениям в информационной сфере и объектов (ЗО) КИИ. Типы нарушений. Статьи. Наказания.	Всего аудиторных часов		
		2	2	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

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	3 Семестр
1	**Тема 1. Сущность организационной ЗКИ. Методы и формы организационной ЗКИ** Способы, источники и методы промышленно-экономического шпионажа.

	Организационные, правовые основы защиты конфиденциальной информации (ЗКИ). Сущность организационной ЗКИ. Методологические основы организации системы ЗКИ. Назначение системы ЗКИ. Принципы построения системы ЗКИ. Стратегия и способы ЗКИ. Каналы утечки конфиденциальной и др. информации. Методы и формы организационной ЗКИ. Классификация организационных мероприятий по ЗКИ.
2	**Тема 2. Подбор персонала и оформление допуска для работы с конфиденциальной информацией. Обучение сотрудников правилам и приёмам работы** Подбор кандидатов. Изучение резюме и изучение кандидатов. Принятие решения руководством на приём. Подписание обязательства о неразглашении тайны фирмы. Предупреждение об ответственности за разглашение конфиденциальной информации. Ознакомление с должностной инструкцией. Изучение личных, моральных и профессиональных качеств сотрудника в течение испытательного срока. Обучение правилам работы с конфиденциальной информацией и документами. Проводение инструктажей, проверка знаний. Анализ результатов работы сотрудника в течение испытательного срока. Оформление допуска к конфиденциальной информации. Выдвигаемые требования (соразмерные с важностью сведений).
3	**Тема 3. Лицензирование деятельности оргвнизаций для проведения работ, связанных с конфиденциальной информацией** Лицензирование деятельности по технической ЗКИ. Термины и определения по ЗКИ. Лицензируемая деятельность. Лицензируемый орган. Лицензируемый сбор. Лицензионные требования, предъявляемые: к соискателю лицензии на осуществление лицензируемого вида деятельности; к лицензиату при осуществлении лицензируемого вида деятельности. Лицензионные требования. Перечень документов, предоставляемых с целью получения лицензии. Получение лицензии.
4	**Тема 4. Режим хранения носителей конфиденциальной информации. Организация физической охраны предприятия, пропускного и внутриобъектового режимов** Носители конфиденциальной информации и их классификация. Виды и уровень угроз безопасности информации в защищаемом момещении. Порядок сдачи под охрану и приём из-под охраны защищаемых и иных помещений и др. Физическая охрана предприятия. Оперативный дежурный на предприятии. Руководитель подразделения личной охраны и его обязанности. Сотрудники подразделения и их обязанности. Система охраны. Методы, меры и способы ЗКИ обеспечивающие нормальную работу предприятия.Пропускной и внутриобъектовый режим предприятия. Оборудование пропускных пунктов и КПП. Допуск на предприятие. Организация внутриобъектового режима.
5	**Тема 5. Организация защиты конфиденциальной информации при проведении закрытых мероприятий** Этапы проведения закрытых совещаний или переговоров. Плановые и внеплановые закрытые совещания или переговоры. Доступ к ним сотрудников организации. Приглашение сторонних лиц на закрытые совещания или переговоры. Ответственность за обеспечение ЗКИ и сохранение тайны организации на совещании. Подготовка закрытого совещания. Оформление списков и организация допуска сторонних лиц на закрытые совещания. Рекламно-выстовочный материал.
6	**Тема 6. Организация защиты конфиденциальной информации при осуществлении международного сотрудничества** Организация работы по обеспечению режима конфиденциальности в связи с предстоящим приёмом иностранцев в данной организации. Разработка, согласование и утверждение программы приёма иностранцеводготовка. Подготовка плана мероприятий. Приём иностранцев. Подведение итогов выполнения запланированных

	режимных мероприятий. Определение персонального состава, привлекаемого к работе с иностранцами. Организация телефонных переговоров. Подготовка производственных помещений. Маршрут передвижения. Подготовка справок в службу безопасности, отражающих вопросы режимного характера.
7	**Тема 7. Организация защиты конфиденциальной продукции в процессе транспортировки** Ответственность транспортников за сохранность перевозимых грузов. Краткий анализ положения дел на транспортных магистралях страны и криминогенная обстановка вокруг. Обеспечение надёжной защиты грузов. Определение маршрутов следования грузов. Численность личного состава охраны. Обеспечение контроля за прохождением груза и выполнение своих обязанностей охраной. Должностные инструкции. Особенности охраны грузов при использовании отдельных видов грузов. Охрана груза перевозимого в купе пассажирского поезда. Охрана груза перевозимого на автомобиле. Использование воздушного транспорта.
8	**Тема 8. Организация служебного расследования по фактам утраты конфиденциальной информации** Разглашение сведений и утрата документов, содержащих КИ. Иные нарушения режима при работе с материалами КИ. Органицация служебного расследования. Назначение председателя и членов комиссии по проведению расследований связанных с нарушением режима и утраты документов КИ. Разработка должностых инструкций дляпредседателя и членов комиссии по проведению расследований связанных с нарушением режима и утраты документов КИ. Сроки проведения расследований и порядок их оформления. Отметка о всех фактах утраты КИ. Порядок оформления журнала учёта утраты КИ.
9	**Тема 9. Теоретические основы информационной безопасности** Нормативно-правовые акты, регулирующие общественные отношения в сфере информационной безопасности. Национальные интересы в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Стратегические цели и основные направления обеспечения информационной безопасности. Понятие и структура информационной безопасности в Российской Федерации. Критическая инфраструктура Российской Федерации.
10	**Тема 10. Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации** Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации Конституционные права граждан в сфере информации. Право на доступ к информации. Общедоступная информация, информация ограниченного доступа. Государственная тайна. Персональные данные. Правовой статус государственных информационных систем. Информационные ресурсы.
11	**Тема 11. Противодействие информационным угрозам** Субъекты и объекты правоотношений в области защиты от информации. Стратегия противодействия экстремизму в Российской Федерации до 2025 года. Полномочия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Федеральный государственный контроль (надзор) за соблюдением требований в связи с распространением информации в информационно-телекоммуникационных сетях, в том числе сети "Интернет". Информация, причиняющая вред здоровью и (или) развитию детей. Информационная продукция для детей разного возраста (не достигших возраста шести лет; достигших возраста шести, двенадцати и шестнадцати лет). Контроль за деятельностью лиц, находящихся под иностранным влиянием.
12	**Тема 12. Государственная политика Российской Федерации в области международной информационной безопасности**

	Основные направления реализации государственной политики в области международной информационной безопасности Механизмы реализации государственной политики в области международной информационной безопасности. Международное законодательство в сфере информационной безопасности. Законодательство зарубежных стран, регулирующее правоотношения в сфере информационной безопасности.
13	**Тема 13. Полномочия прокурора в сфере ограничения доступа к информации, распространяемой с нарушением закона и основные принципы организации информационной безопасности в органах прокуратуры** Полномочия органов прокуратуры Российской Федерации по противодействию экстремизму в информационной сфере. Информационная безопасность как один из базовых принципов цифровой трансформации органов прокуратуры Российской Федерации. Основные принципы организации информационной безопасности в органах прокуратуры Российской Федерации.
14	**Тема 14. Защита интеллектуальных прав и ответственность за правонарушения в сфере информации** Объекты и субъекты авторского права. Исключительные авторские права. Смежные права. Ответственность за правонарушения в информационной сфере. Общая характеристика и виды ответственности за правонарушения в информационной сфере. Уголовная ответственность в информационной сфере. Административная ответственность в информационной сфере. Дисциплинарная ответственность в информационной сфере. Материальная ответственность в информационной сфере.
15	**Тема 15. Нормативное регулирование и ответственность субъектов КИИ** Полномочия федеральных органов исполнительной власти в сфере обеспечения безопасности ЗО КИИ. Штрафы и установленные сроки давности привлечения к административной ответственности за нарушения в области обеспечения безопасности КИИ РФ. Признание правонарушений с длящимся сроком давности (с момента обнаружения правонарушения проверяющим). Нормативные правовые акты (НПА) в области обеспечения безопасности значимых объектов (ЗО) КИИ и ИБ. Типы нарушений, статьи и наказания в области обеспечения безопасности значимых объектов (ЗО) КИИ и ИБ.
16	**Тема 16. Актуальные проблемы правового и организационного обеспечения ИБ. Особенности организационно-правового обеспечения защиты информационных систем** Противодействие экстремистской деятельности в информационной сфере. Защита детей от информации, причиняющей вред их здоровью и развитию. Правовые проблемы обеспечения информационной безопасности в сети Интернет. Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства. Практика разработки и реализации политики информационной безопасности корпоративных информационных систем.

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 организации и управления, 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 технической защиты конфиденциальной информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на практических и семинарских 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-8	З-ПК-8	ЗО, КИ-8, КИ-16
	У-ПК-8	ЗО, КИ-8, КИ-16
	В-ПК-8	ЗО, КИ-8, 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 существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Т 83 Защита информации на предприятии : учебное пособие, Петровский М. В., Тумбинская М. В., Санкт-Петербург: Лань, 2020

2. ЭИ Н 62 Методы защиты информации. Защита от внешних вторжений : , Никифоров С. Н., Санкт-Петербург: Лань, 2022

3. ЭИ П 54 Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов, Полякова Т. А., Москва: Юрайт, 2022

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 621.39 Б 90 Выявление специальных технических средств несанкционированного получения информации : , Бузов Г.А., Москва: Горячая линия - Телеком, 2019

2. 004 Б90 Защита от утечки информации по техническим каналам : учеб. пособие, Кондратьев А.В., Бузов Г.А., Калинин С.В., М.: Горячая линия - Телеком, 2005

3. 004 П30 Основы практической защиты информации : , Петраков А.В., М.: Радио и связь, 1999

4. 65 Б90 Что такое управление? Кто такой руководитель? Кн.1 Система управления, Булыгин Ю.Е., М.: Русское слово, 2004

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 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 информационной безопасности и защиты информации, организационно-распорядительные, нормативные и информационные документы ФСБ России, 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, являющихся основами технической защиты конфиденциальной информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы.

В качестве форм промежуточного контроля полученных знаний (раздел 1 и 2) используются: контрольная работа и тестирование. Для повышения результатов контроля студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты).

В процессе итогового контроля также могут использоваться результаты, полученные студентами на практических занятиях.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

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

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы – «Обеспечение безопасности 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 технической защиты конфиденциальной информации, организационно-распорядительные, нормативные и информационные документы ФСБ России, 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, являющихся основами технической защиты конфиденциальной информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических работ по отработке практических навыков использования математических методов и программных средств технической защиты информации. Результаты, полученные в ходе практических работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний (раздел 1 и 2) используются: контрольная работа и тестирование. Для повышения результатов контроля студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты).

В процессе итогового контроля также могут использоваться результаты, полученные студентами на практических занятиях.

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 экзамен или зачёт.

2. Указания по контролю самостоятельной работы студентов.

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

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

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

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

Автор(ы):

Марченко Анатолий Васильевич

Рецензент(ы):

Дураковский А.П.