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

КОМПЛЕКСНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

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	2	72	16	16	0		40	0	З
Итого	2	72	16	16	0	2	40	0	

АННОТАЦИЯ

Цель дисциплины - обеспечение требуемого уровня знаний, умений и навыков у студентов структуры, логической организации, системы управления службой защиты информации как основного звена систем защиты информации.

Дисциплина «Комплексные системы защиты информации на предприятии» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом (ФГОС3++), содействует формированию научного мировоззрения и системного мышления; посвящена изучению основ комплексной системы защиты информации на предприятии. Именно глубокое изучение организационных основ и управления должно сформировать устойчивые навыки использование законодательства, задающего нормативно-правовую базу, являющуюся необходимым элементом управленческой деятельности и организационного обеспечения информационной безопасности.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является формирование общих представлений о принципах защиты (службой безопасности) информации, лежащих в основе применения организационных и управленческих методов защиты информации.

Учебная дисциплина «Комплексные системы защиты информации на предприятии» относится к разделу общеобразовательных дисциплин, логически и содержательно-методически взаимосвязанной с такими дисциплинами как «Правоведение», и «Организационное и правовое обеспечение информационной безопасности». Именно глубокое изучение основ правоведения должно сформировать устойчивые навыки использование законодательства, задающего нормативно-правовую базу, являющуюся необходимым элементом управленческой деятельности и организационного обеспечения информационной безопасности.

Задачи дисциплины - это определение места службы защиты информации в системе безопасности предприятия; объяснение функций службы защиты информации; обоснование оптимальной структуры и штатного состава службы защиты информации в зависимости от решаемых задач и выполняемых функций; установление организационных основ и принципов деятельности службы защиты информации; разрешение общих и специфических вопросов подбора, расстановки и обучения кадров, организации труда сотрудников службы защиты информации; раскрытие принципов, методов и технологии управления службой защиты информации.

В результате обучения студенты должны ознакомиться с:

целями, задачами и принципами комплексной системы защиты информации;

перспективными направлениями развития технических средств разведки и систем охраны объектов;

принципами организации работ по компьютерной защите информации;

основными демаскирующими признаками объектов защиты и носителей информации;

техническими каналами утечки информации; техническими средствами разведки;

способами и средствами защиты конфиденциальной информации;

основными руководящими документами по защите предприятий и учреждений от иностранной технической разведки;

моделированием объектов защиты;

определением рациональных управленческих и организационных мер по комплексной защите информации и оцениванием их эффективности;

ведением контроля эффективности мер по защите объектов;

формальной постановкой и решением задач эффективного применения средств и систем защиты информации;

применением полученных знаний на практике.

Вместе с другими дисциплинами общенаучного и профессионального циклов дисциплин изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как:

строгость в суждениях,

творческое мышление,

организованность и работоспособность,

дисциплинированность,

самостоятельность и ответственность.

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 «Комплексные системы защиты информации на предприятии» студенты должны знать следующие дисциплины: «Математический анализ»; «Теория вероятностей и математическая статистика»; «Общая алгебра»; «Линейная алгебра»; «Дискретная математика»; «Информатика»; «Теория информации»; «Основы информационной безопасности».

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

знать структуру, логической организации, системы управления службой защиты информации как основного звена систем защиты информации;

уметь применять знания, навыки и умения в области организации и управления службой защиты информации на предприятии;

владеть навыками ведения организационных и управленческих мероприятий по защите информации на предприятии.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-1 [1] – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее	В-ОПК-1 [1] – Владеть: навыками участия в разработке системы обеспечения информационной безопасности объекта; навыками проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности У-ОПК-1 [1] – Уметь: проектировать информационные

создание	системы; обосновывать и планировать состав и архитектуру моделируемых и проектируемых информационных, автоматизированных и автоматических систем; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности. З-ОПК-1 [1] – Знать: основы стандартов в области обеспечения информационной безопасности; элементы компьютерного моделирования сложных систем, проектирования информационных, автоматизированных и автоматических систем
ОПК-2 [1] – Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	З-ОПК-2 [1] – Знать: методы проектирования технологий обеспечения информационной безопасности; принципы построения и функционирования современных информационных систем; требования к системам комплексной защиты информации У-ОПК-2 [1] – Уметь: обосновывать применяемые методы решения задач защиты информации, проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов, разрабатывать модели угроз и нарушителей информационной безопасности В-ОПК-2 [1] – Владеть: навыками проектирования систем информационной безопасности
УК-1 [1] – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	З-УК-1 [1] – Знать: методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации У-УК-1 [1] – Уметь: применять методы системного подхода и критического анализа проблемных ситуаций; разрабатывать стратегию действий, принимать конкретные решения для ее реализации В-УК-1 [1] – Владеть: методологией системного и критического анализа проблемных ситуаций; методиками постановки цели, определения способов ее достижения, разработки стратегий действий

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	Средства и технологии обеспечения	ПК-1 [1] - Способен принимать участие в разработке систем	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики

безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	безопасности значимых объектов критической информационной инфраструктуры	обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.030, 06.032, 06.033, 06.034	оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи;

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

			обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных 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.

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	Глава 1. Введение в основы комплексной системы защиты информации. Глава 2. Информационное противоборство.	1-8	8/8/0		25	КИ-8	З-ПК-1, У-ПК-1, З-ПК-2, У-ПК-2, З-УК-1, У-УК-1, З-ОПК-1, У-ОПК-1, З-

							ОПК-2, У-ОПК-2
2	Глава 3. Введение в информационную безопасность предприятия. Глава 4. Организация деятельности службы безопасности в организации.	9-16	8/8/0		25	КИ-16	В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-1, У-УК-1, В-УК-1, З-ОПК-1, У-ОПК-1
	Итого за 3 Семестр		16/16/0		50		
	Контрольные мероприятия за 3 Семестр				50	З	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2,

							В-ПК-2, З-УК-1, У-УК-1, В-УК-1, З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2

* – 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.**
	3 Семестр	16	16	0
1-8	**Глава 1. Введение в основы комплексной системы защиты информации. Глава 2. Информационное противоборство.**	8	8	0
1 - 4	**Введение в основы комплексной системы защиты информации**	Всего аудиторных часов		
		4	4	0
	Тема 1. Введение в дисциплину «Комплексные системы защиты информации на предприятии». Предмет и задачи дисциплины «Комплексные системы защиты информации	Онлайн		
		0	0	0

	на предприятии». Исторический очерк о возникновении органов защиты информации и службы защиты информации на предприятиях. Концептуальные основы информационной безопасности. Информационная безопасность в Российской Федерации (РФ). Правовые, организационные и управленческие основы защиты информации. Тема 2. Методологические основы организации системы защиты информации. Методология защиты информации (ЗИ) как теоретический базис системы защиты информации. Подходы к проектированию систем защиты информации организации. Основные направления и принципы обеспечения комплексной безопасности объектов информатизации. Понятие и назначение системы защиты информации. Стратегия и принципы построения системы защиты информации. Выработка политики безопасности. Тема 3. Методологические основы обеспечения комплексной безопасности объектов информации. Алгоритм разработки системы обеспечения комплексной безопасности объекта (информатизации). Определение возможного ущерба объекту при реализации наиболее вероятных угроз. База данных угроз ФСТЭК России. Анализ способов защиты от угроз безопасности объекту информатизации. Оценка эффективности комплексной системы защиты объектов. Тема 4. Разработка концепции и создание системы обеспечения (комплексной) безопасности объекта информатизации. Разработка концепции обеспечения комплексной безопасности: постановка задач. Методика разработки концепции безопасности и план мероприятий по её реализации. Порядок внедрения системы обеспечения комплексной безопасности на объектах информатизации. Функциональные системы обеспечения комплексной безопасности в условиях нештатных и чрезвычайных ситуациях.			
5 - 8	**Информационное противоборство** Тема 5. Информационное противоборство и радиоэлектронная борьба как средство информационного противоборства. Сущность и содержание информационного противоборства. Анализ методов и технологий информационного противоборства. Радиоэлектронная борьба: цели и задачи. Радиоэлектронная разведка. Радиоэлектронное подавление и защита. Средства оптико-электронного подавления. Тема 6. Разведывательные службы по несанкционированному доступу к защищаемой информации: направления, виды, деятельность. Государственные разведывательные органы. Цели и задачи разведки. Разведывательная деятельность: направления и виды. Деятельность разведывательных органов, технической разведки. Оценка возможностей технической	Всего аудиторных часов		
		4	4	0
		Онлайн		
		0	0	0

	разведки по добыванию информации. Особенности несанкционированного доступа к ЗИ со стороны преступного мира и коммерческих организаций. Тема 7. Противодействие техническим разведкам и техническая защита конфиденциальной информации. Основные методы технической разведки. Методы защиты информации от технических разведок. Противодействие техническим разведкам и техническая защита конфиденциальной информации (ТЗКИ). Применение технических средств и систем защиты информации от шпионажа. Организационные аспекты ТКЗИ. Тема 8. Противодействие техническим разведкам и физическая защита объекта. Системы контроля и управления доступом (СКУД). Назначение, классификация и состав СКУД. Идентификатор пользователя. Контроллеры. Устройства идентификации личности (считыватели). Исполнительные устройства. Средства идентификации (аутентификации) и их классификация. Средства биометрической идентификации личности. Основные характеристики средств биометрической идентификации личности.			
9-16	**Глава 3. Введение в информационную безопасность предприятия. Глава 4. Организация деятельности службы безопасности в организации.**	8	8	0
9 - 12	**Введение в информационную безопасность предприятия** Тема 9. Информационная безопасность предприятия. Системный подход к обеспечению информационной безопасности. Основные требования, предъявляемые к системе защиты информации (ЗИ). Стратегия защиты информации. Подходы к проектированию систем защиты информации. Понятие системы защиты информации. Назначение системы защиты информации. Принципы построения системы защиты информации. Тема 10. Подразделения обеспечения безопасности. Виды, требования и задачи охраны. Структура подразделений обеспечения безопасности. Особенности охраны объектов на различных этапах строительства. Отбор, профессиональная подготовка и переподготовка сотрудников подразделения обеспечения безопасности в организации. Изучение сотрудников в процессе работы. Тема 11. Организация службы безопасности предприятия. Задачи службы безопасности. Служба безопасности предприятия: структура и организация деятельности. Организация внутриобъектового режима на объекте организации. Технические системы охранной сигнализации объектов защиты. Проверка наличия конфиденциальных документов, дел и носителей информации. Тема 12. Организация деятельности службы безопасности. Организация безопасного функционирования информационных систем на объекте предприятия. Организация инженерно-технической защиты объекта	Всего аудиторных часов 4 Онлайн 0	4 0	0 0

	информатизации. Организация служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа. Проведение аналитико-разведывательной работы службой безопасности.			
13 - 16	**Организация деятельности службы безопасности предприятия** Тема 13. Планирование мероприятий и управление системой защиты объектов. Управление системой защиты объектов. Организация внутриобъектового и пропускного режимов в организации. Организация технической защиты информации на объектах информатизации. Интегрированные и комплексные системы безопасности. Инженерно-техническая защита объектов. Методы и средства технической защиты информации. Проектирование системы физической защиты объекта. Тема 14. Обеспечение охранной и пожарной безопасности объектов. Обеспечение охранной безопасности объектов: правовые и организационные аспекты. Технические средства обеспечения охранной безопасности на объекте. Обнаружение проникновения на объект. Обеспечение защитных мер в случае проникновения злоумышленника на объект защиты. Обеспечение пожарной безопасности объектов: правовые и организационные аспекты. Технические средства обеспечения пожарной безопасности на объекте. Обнаружение пожара на объекте. Обеспечение пожаротушения на объекте. Обеспечение эвакуации и спасение людей на объекте при возникновении пожара. Автоматизированные системы управления противопожарной защитой объекта. Тема 15-16. Управление системой защиты информации в условиях чрезвычайных ситуаций. Понятие и виды чрезвычайных ситуаций. Технология принятия решения в условиях чрезвычайных ситуаций. Факторы, влияющие на принятие решений. Подготовка мероприятий службой безопасности организации на случай возникновения чрезвычайной ситуации. Планирование и контроль деятельности службой безопасности. Антитеррористическая деятельность по защите объектов информатизации. Основы антитеррористической деятельности в организации. Взрывные устройства и меры борьбы с ними. Средства обнаружения взрывных устройств и взрывных веществ на объектах. Средства предотвращения взрывов на объектах. Средства разминирования и защиты от опасных факторов вызывающих взрывы на объектах.	Всего аудиторных часов		
		4	4	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 - 4	**Введение в основы комплексной системы защиты информации** Введение в дисциплину «Комплексные системы защиты информации на предприятии». Методологические основы организации системы защиты информации. Методологические основы обеспечения комплексной безопасности объектов информации. Разработка концепции и создание системы обеспечения (комплексной) безопасности объекта информатизации.
5 - 8	**Информационное противоборство** Информационное противоборство и радиоэлектронная борьба как средство информационного противоборства. Разведывательные службы по несанкционированному доступу к защищаемой информации: направления, виды, деятельность. Противодействие техническим разведкам и техническая защита конфиденциальной информации. Противодействие техническим разведкам и физическая защита объекта. Системы контроля и управления доступом (СКУД).
9 - 12	**Введение в информационную безопасность предприятия** Информационная безопасность предприятия. Подразделения обеспечения безопасности. Организация службы безопасности предприятия. Организация деятельности службы безопасности.
13 - 16	**Организация деятельности службы безопасности в организации** Планирование мероприятий и управление системой защиты объектов. Обеспечение охранной и пожарной безопасности объектов. Управление системой защиты информации в условиях чрезвычайных ситуаций. Антитеррористическая деятельность по защите объектов информатизации.

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.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	**Индикаторы освоения**	**Аттестационное мероприятие (КП 1)**
ОПК-1	З-ОПК-1	З, КИ-8, КИ-16
	У-ОПК-1	З, КИ-8, КИ-16
	В-ОПК-1	З, КИ-16
ОПК-2	З-ОПК-2	З, КИ-8, КИ-16
	У-ОПК-2	З, КИ-8, КИ-16
	В-ОПК-2	З, КИ-16
ПК-1	З-ПК-1	З, КИ-8, КИ-16
	У-ПК-1	З, КИ-8, КИ-16
	В-ПК-1	З, КИ-16
ПК-2	З-ПК-2	З, КИ-8, КИ-16
	У-ПК-2	З, КИ-8, КИ-16
	В-ПК-2	З, КИ-16
УК-1	З-УК-1	З, КИ-8, КИ-16
	У-УК-1	З, КИ-8, КИ-16
	В-УК-1	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 Т 83 Защита информации на предприятии : учебное пособие, Санкт-Петербург: Лань, 2020

2. ЭИ К 77 Методы защиты информации : учебное пособие, Санкт-Петербург: Лань, 2021

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

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 65 Б90 Что такое управление? Кто такой руководитель? Кн.1 Система управления, , 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 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.

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):

Дураковский Анатолий Петрович, к.т.н., доцент

Рецензент(ы):
Горбатов В.С.