

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
МОДЕЛИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

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, экс./зач./КР/КП
2, 4	2	72	30	0	0		42	0	3
Итого	2	72	30	0	0	0	42	0	

АННОТАЦИЯ

Изучение дисциплины «Моделирование систем защиты информации» предполагает изучение основных понятий, принципов и особенностей технологий построения защищенных автоматизированных систем (АС) с учетом возрастающей в мире роли России, в том числе в мировой атомной энергетике.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель курса состоит в формировании у студентов знаний основ технологии построения, проектирования и создания защищенных автоматизированных систем, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

Задачи дисциплины:

- изучить концепции обеспечения информационной безопасности автоматизированных систем;
- познакомить с технологиями функционирования защищенной автоматизированной системы;
- изучить методологии оценки защищенности автоматизированных систем;
- сформировать представление о принципах построения защищенных информационных систем;
- дать информацию об основополагающих нормативно-правовых актах в области обеспечения информационной безопасности автоматизированных систем.

В курсе рассматриваются следующие темы:

- системная инженерия;
- защищенные автоматизированные системы;
- жизненный цикл системы;
- порядок выполнения работ по проектированию и созданию систем;
- техническая документация;
- основы оценки соответствия;
- критическая информационная инфраструктура.

Значительное место отведено методам оценки соответствия средств защиты информации и защищенности автоматизированных систем, которым в современных технологиях уделяется повышенное внимание.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

В процессе изучения дисциплины студенты получают возможность последовательно рассмотреть технологии и систему построения защищенных автоматизированных систем и её основные элементы и др. От студентов требуется знание основ защиты информации. Дисциплина «Технология построения защищенных автоматизированных систем» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры». Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико-математической подготовкой, знаниями и умениями

основ информационных технологий, автоматизированных систем и информационной безопасности.

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 соответствии 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 [1] - Способен определять объекты КИИ, готовить перечни объектов КИИ, подлежащие категорированию <i>Основание:</i> Профессиональный стандарт: 06.030, 06.034	3-ПК-2.1[1] - Знать: Основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов; Принципы построения АСУ ТП АЭС и критические процессы, происходящие в результате штатной работы. ; У-ПК-2.1[1] - Уметь: Выявлять и собирать сведения о критических процессах в АСУ, информационных и телекоммуникационных системах, в частности в АСУ ТП АЭС; Определять категории

			<p>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.</p>
<p>Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации</p>	<p>Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры</p>	<p>ПК-2.3 [1] - Способен устанавливать требования к обеспечению безопасности значимого объекта КИИ, осуществлять выбор и реализацию мер по обеспечению безопасности значимых объектов КИИ</p> <p><i>Основание:</i> Профессиональный стандарт: 06.033, 06.034</p>	<p>З-ПК-2.3[1] - Знать: Отечественные стандарты в области информатизации и обеспечения информационной безопасности АСУ, информационных и телекоммуникационных систем общего и специального назначения; Основные принципы обеспечения безопасности КИИ; Основные положения ядерной безопасности; Причины возникновения инцидентов ядерной безопасности; Основные виды угроз</p>

			<p>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</p>
--	--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

			<p>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.</p>
контрольно-аналитический			
<p>Контроль защищенности ЗО КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации</p>	<p>Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, обеспечивающие безопасность критических процессов значимых объектов критической информационной инфраструктуры</p>	<p>ПК-4 [1] - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности</p> <p><i>Основание:</i> Профессиональный стандарт: 06.032, 06.034</p>	<p>3-ПК-4[1] - Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от</p>

			<p>несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие требованиям по безопасности информации. ; У-ПК-4[1] - Уметь: оценивать эффективность защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему</p>
--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

			<p>с целью определения уровня защищенности и доверия; применять инструментальные средства проведения сертификационных испытаний; разрабатывать программы и методики сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; проводить экспертизу технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4[1] - Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем</p>
--	--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

			и сетей; основами подготовки протоколов испытаний и технического заключения по результатам сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.
--	--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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
	<i>2 Семестр</i>						
1	Методологические основы моделирования	1-8	16/0/0		25	КИ-8	3-ПК-2.1, У-ПК-2.1, В-ПК-2.1,

							3-ПК-2.3, У-ПК-2.3, В-ПК-2.3, 3-ПК-4, У-ПК-4, В-ПК-4
2	Модели безопасности и их применение	9-15	14/0/0		25	КИ-15	3-ПК-2.1, У-ПК-2.1, В-ПК-2.1, 3-ПК-2.3, У-ПК-2.3, В-ПК-2.3, 3-ПК-4, У-ПК-4, В-ПК-4
	<i>Итого за 2 Семестр</i>		30/0/0		50		
	Контрольные мероприятия за 2 Семестр				50	3	3-ПК-2.1, У-ПК-2.1, В-ПК-2.1, 3-ПК-2.3, У-ПК-2.3, В-ПК-

							2,3, 3-ПК- 4, У- ПК-4, В- ПК-4
--	--	--	--	--	--	--	--------------------------------------------------

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	<i>2 Семестр</i>	30	0	0
1-8	Методологические основы моделирования	16	0	0
1 - 2	1. Введение Основные понятия, понятие модели, цели и задачи моделирования, классификация моделей систем и процессов защиты информации, анализ развития методов моделирования систем и процессов защиты информации, общие модели защиты. Свойства моделей безопасности, их практические приложения. Базовая модель нарушителя. Классические модели защиты информации от НСД.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
3 - 4	2. Методологические основы моделирования Основы общей методологии моделирования, аналитическое и статистическое моделирование; особенности моделирования систем и процессов защиты информации. Необходимость расширения методов моделирования, разработанных в рамках классической теории систем. Содержание этапов моделирования, компоненты моделирования. Основные направления развития методов моделирования: основные положения теории игр, теории СМО, теории нечетких множеств, лингвистических переменных, вероятностно-автоматного моделирования, методов экспертных оценок. Методы измерений, обработка мнений экспертов методом ранжирования.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
5 - 6	2. Методологические основы моделирования Оценка результата экспертизы, методика предварительной оценки риска. Аксиомы полезности. Определение и виды шкал измерений Понятие нечеткого подмножества,	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0

	лингвистической переменной, практическое приложение теории нечетких подмножеств. Операции над нечеткими подмножествами, понятие нечеткой вероятности и ее свойства. Нечеткие отношения и операции над ними, нечеткие графы, нечеткие алгоритмы. Шкалирование нечетких оценок. Понятие задачи принятия решений, подход Беллмана-Заде. Лингвистическая модель задачи принятия решений, понятие нечеткой функции, принцип обобщения. Модель коллективного принятия решений, Теорема Эрроу. Свойства моделей безопасности, их практические приложения.			
7	3. Методы и технологии построения моделей Сущность методологии структурного анализа и проектирования, два подхода к моделированию. Методы декомпозиции, пример. Методика SADT - моделирования, оценка результата. Правила построения SADT - диаграмм. Правила декомпозиции ограниченных объектов, определения конца моделирования, применение SADT - моделирования.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
8	4. Модели безопасности Модель АДЕПТ-50. Матричная модель Харрисона. Модель безопасности Клементса (с полным перекрытием). Модель Хартсона (пятимерное пространство). Модель Дэннинг (решетчатая модель информационных потоков).	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
9-15	Модели безопасности и их применение	14	0	0
9 - 10	4. Модели безопасности Понятие информационного потока, виды потоков,. Изменение состояния и информационный поток. Моделирование создания и уничтожения субъектов и объектов. Операция изменения значения и класса секретности объекта. Правила информационного потока. Решетчатая структура. Анализ потоков, проверка допустимости потоков, монитор обращений. Модель Белла -Ла Падулы (модель состояний). Модель Take-Grant, теорема 1 (гарантии доступа), теорема 2 (необходимые и достаточные условия доступа). Формальная спецификация и верификация моделей. Определение соответствия спецификаций модели (техника). Модели конечных состояний , шаги построения модели. Стоимостная модель оценки затрат Терна. Основные положения нормативных документов ГТК России, требования по защите информации.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
11 - 12	5. Применение Моделей Методика построения модели с использованием технологии SADT. Модели анализа. Сущность анализа риска,. Модели анализа уязвимости информации: общая постановка задачи оценки уязвимости (защищенности) информации. Эмпирические модели оценки; теоретико-вероятностные модели оценки; модели прогнозирования значений показателей уязвимости информации.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0

	Модели синтеза. Модели синтеза систем защиты информации (СЗИ): постановка задачи, особенности и этапы синтеза СЗИ, задачи структурного и параметрического синтеза СЗИ. Общая модель оптимизации СЗИ. Модели проектирования СЗИ на базе типовых проектных решений.			
13 - 14	5. Применение Моделей Модели проектирования уникальных СЗИ. Модели управления. Модели управления СЗИ: цели и задачи управления СЗИ; общая модель технологии управления СЗИ; модель планирования защиты информации; модель оперативно-диспетчерского управления защитой; модель календарного руководства выполнением планов защиты информации; модель информационного обеспечения повседневной деятельности органов защиты информации. Взаимосвязь моделей и связь с этапами жизненного цикла систем защиты. Получение информации с помощью моделей и ее интерпретация.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
15	6. Организация разработки и практической реализации моделей защиты информации Организация разработки и практической реализации моделей защиты информации; основные процессы разработки и реализации; структура, содержание и организация рабочего инструментария моделирования систем и процессов защиты; перспективы и проблемы формирования рабочего инструментария моделирования.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	Полное наименование
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с целью формирования и развития профессиональных навыков студентов и требованиями ОС ВО НИЯУ МИФИ по направлению подготовки реализация компетентного подхода предусматривает в учебном процессе широкое использование активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой.

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

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-2.1	З-ПК-2.1	З, КИ-8, КИ-15
	У-ПК-2.1	З, КИ-8, КИ-15
	В-ПК-2.1	З, КИ-8, КИ-15
ПК-2.3	З-ПК-2.3	З, КИ-8, КИ-15
	В-ПК-2.3	З, КИ-8, КИ-15
	У-ПК-2.3	З, КИ-8, КИ-15
ПК-4	З-ПК-4	З, КИ-8, КИ-15
	В-ПК-4	З, КИ-8, КИ-15
	У-ПК-4	З, КИ-8, КИ-15

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

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			Оценка «удовлетворительно» выставляется студенту, если он имеет

60-64	«удовлетворительно»	Е	знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
Ниже 60	2 – «неудовлетворительно»	Ф	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 41 Надежность технических систем и техногенный риск : учебник и практикум для вузов, Москва: Юрайт, 2022
2. ЭИ Г 16 Организация и безопасность дорожного движения : учебник для вузов, Москва: Юрайт, 2022
3. 681.3 Г37 Защита информации в автоматизированных системах обработки данных Кн.1 , , М.: Энергоатомиздат, 1994
4. 629 Т47 Моделирование при обеспечении безопасности космических полетов : , А. А. Тищенко, В. И. Ярополов, Москва: Машиностроение, 1981
5. 004 Г37 Основы защиты информации : Учебник для вузов, В. А. Герасименко, А. А. Малюк, М.: МИФИ, 1997

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. www.fstec.ru; www.gost.ru; www.fsb.ru. ()
2. <http://www.jetinfo.ru> ()
3. <http://www.scinet.cc> ()

4. <https://bit.spels.ru/index.php/bit> ()

5. <http://www.cerias.purdue.edu/> ()

6. <http://www.securityfocus.com/> ()

<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

Методические рекомендации студентам по изучению дисциплины «Моделирование систем защиты информации»

Методические рекомендации по организации работы студента на лекциях

Во время лекции по дисциплине «Моделирование систем защиты информации» студент должен уметь сконцентрировать внимание на рассматриваемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого ему необходимо конспектировать материал, излагаемый преподавателем. Во время конспектирования в работу включается моторно-двигательная память, позволяющая эффективно усвоить лекционный материал. Весь иллюстративный материал, представляемый на лекции (на слайдах, на доске, в раздаточном материале) также должен быть зафиксирован в конспекте лекций. Каждому студенту необходимо помнить о том, что конспектирование лекции – это не диктант. Студент должен уметь (или учиться уметь) выделять главное и фиксировать основные моменты «своими словами». Это гораздо более эффективно, чем запись «под диктовку».

На лекциях по дисциплине «Моделирование систем защиты информации» периодически проводится письменный опрос (тестирование) студентов по материалам лекций. Подборка вопросов осуществляется на основе изученного теоретического материала. Такой подход позволяет не только контролировать уровень усвоения теоретического материала, но и организовать эффективный контроль посещаемости занятий на лекциях.

Методические рекомендации по организации работы студента на семинарских занятиях

По курсу «Моделирование систем защиты информации» важное место в учебном процессе занимают семинарские занятия, призванные закреплять полученные студентами теоретические знания.

Перед семинарским занятием студенту необходимо восстановить в памяти теоретический материал по теме семинарского занятия. Для этого следует обратиться к соответствующим конспекту лекций, главам учебника, настоящим методическим указаниям.

Каждое занятие начинается с повторения теоретического материала по соответствующей теме. Студенты должны уметь чётко ответить на вопросы, поставленные преподавателем. По характеру ответов преподаватель делает вывод о том, насколько тот или иной студент готов к продолжению освоения курса.

После такой проверки студентам предлагается выполнить соответствующие задания и задачи. Что касается типов задач, решаемых на семинарских занятиях, то это различные ситуационные задачи на усвоение студентами теоретического материала.

Порядок решения задач студентами может быть различным. Преподаватель может установить такой порядок, согласно которому каждый студент в отдельности самостоятельно решает задачу без обращения к каким – либо материалам или к преподавателю. Может быть использован и такой порядок решения задачи, когда предусматривается самостоятельное решение каждым студентом поставленной задачи с использованием конспектов, учебников и других методических и справочных материалов. При этом преподаватель обходит студентов, наблюдая за ходом решения и давая индивидуальные указания.

В конце занятия преподаватель подводит его итоги, даёт оценку активности студентов и уровня их знаний.

Методические рекомендации по организации самостоятельной работы студента

Для эффективного достижения указанных выше целей обучения по дисциплине «Моделирование систем защиты информации» процесс изучения материала курса предполагает достаточно интенсивную работу не только на лекциях и семинарах, но и с различными текстами и информационными ресурсами в ходе самостоятельной работы.

Самостоятельная работа по дисциплине «Моделирование систем защиты информации» делится на аудиторную и внеаудиторную. Вопросы организации самостоятельной работы в ходе аудиторных занятий рассмотрены в предыдущих разделах предлагаемых методических рекомендаций. Поэтому рассмотрим процесс организации самостоятельной внеаудиторной работы студентов. Весь материал темы или отдельных ее вопросов, выносимых на самостоятельное изучение, разбивается на небольшие части. В конце каждой части приводятся вопросы для самоконтроля, отвечая на которые студент может проверить степень усвоения им изучаемого материала. Внеаудиторная самостоятельная работа включает также выполнение индивидуальных контрольных заданий. По результатам работы студента на практических занятиях проставляется оценка в ведомость текущего контроля успеваемости и посещаемости студентов, а также передаются сведения в автоматизированную систему контроля самостоятельной и аудиторной работы студентов в Учебный Департамент НИЯУ «МИФИ».

Подготовка к зачету и порядок его проведения

Итоговой формой контроля знаний студентов в семестре по дисциплине «Моделирование систем защиты информации» является зачет. Перед проведением зачета студенту необходимо восстановить в памяти теоретический материал по всем темам курса. Для этого следует обратиться к соответствующим конспекту лекций, главам учебника и другим источникам. Зачет по курсу «Моделирование систем защиты информации» может быть проведен в традиционной устной форме, но с обязательной записью основных формулировок по каждому вопросу в зачетном листе. Данный лист может служить документом при подаче апелляции. В качестве методической помощи студентам при подготовке к зачету рекомендуется перечень вопросов для подготовки к зачету. Зачет по курсу может быть проведен также в письменной форме: в форме письменных ответов на вопросы (на усмотрение преподавателя). Вопросы должны в обязательном порядке охватывать все дидактические единицы дисциплины «Моделирование систем защиты информации». Форма проведения зачета сообщается студентам на последних занятиях.

Зачет определяется на основе суммы баллов, полученных по всем разделам по результатам самостоятельной работы при условии, что студент по каждому виду набрал

количество баллов не менее зачетного минимума. Так зачет проставляется если студент в сумме набрал от 60-100 баллов. Неудовлетворительно - ниже 60 баллов.

Сумма баллов Оценка (ECTS) Градация

90 - 100 А отлично

85 - 89 В очень хорошо

75 - 84 С хорошо

70 - 74 D хорошо

65 - 69 D удовлетворительно

60 - 64 E удовлетворительно

Ниже 60 F неудовлетворительно

В основу разработки данной бально-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости студентов основана на использовании совокупности контрольных точек, оптимально расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Методические рекомендации для преподавателя по организации изучения дисциплины «Моделирование систем защиты информации»

Целью методических рекомендаций являются формирование теоретико-методологических знаний и закрепление профессиональных навыков в области построения, проектирования и создания защищенных автоматизированных систем, а также навыков и умения в применении знаний для конкретных условий.

Методологические подходы к изучению дисциплины «Моделирование систем защиты информации»

- Направленность обучения на получение студентами качественных знаний, которые являются средством развития мышления и культуры, основой воспитания и поведения, будущего практического применения в различных сферах профессиональной деятельности.

- Реализация возможностей студентов в процессе выявления дискуссионных вопросов и комплексных проблем, определения взаимосвязей, анализа разнообразной информации.

- Развитие самостоятельности и способности принятия эффективных решений, определения выбора тех или иных действий с точки зрения их результативности.

Средства обеспечения освоения дисциплины «Моделирование систем защиты информации»

Общий подход к реализации всего программного комплекса предполагает широкое использование активных методических форм преподавания материала.

Необходимо также обратить внимание на сочетание различных форм и методов обучения, включая лекционную форму подачи наиболее фундаментальных положений, изложение доступного материала в виде непрерывного диалога, проведение практикумов, закрепляющих полученные теоретические знания посредством конкретных расчетов и принятия решений.

При изучении курса рекомендуется широко использовать наглядные пособия, презентации, фрагменты учебных кинофильмов по отдельным разделам дисциплины и обучающие программы.

Формы проведения учебных занятий:

- Практикумы (теоретические и практические задания).
- Ситуационные (творческие) задачи, вопросы для обсуждения (закрепление представлений учащихся об экономических понятиях и явлениях, навыков формирования конструктивных и конкретных вопросов).
- Тестовые задания (тестирование).

Педагогические функции преподавания дисциплины реализуются через совокупность педагогических приемов. В качестве основных можно выделить следующие:

Дидактические (способность к передаче знаний в краткой и интересной форме, т. е. умение делать учебный материал доступным для студентов, опираясь на взаимосвязь теории и практики, учебного материала и реальной экономической действительности).

Рефлексивно-гностические (способность понимать студентов, базирующаяся на интересе к ним и личной наблюдательности; самостоятельный и творческий склад мышления; находчивость или быстрая и точная ориентировка).

Интерактивно-коммуникативные (педагогически волевое влияние на студентов, требовательность, педагогический такт, организаторские способности, необходимые как для обеспечения работы самого преподавателя, так и для создания хорошего психологического климата в учебной группе).

Речевые (содержательность, яркость, образность и убедительность речи преподавателя; способность ясно и четко выражать свои мысли и чувства с помощью речи, а также мимики и жестов).

Материально-техническое обеспечение дисциплины «Моделирование систем защиты информации»

При выполнении заданий, самостоятельных работ и подготовке учебно-методических комплексов предусматривается применение ПК. Возможно обращение к сети Интернет.

Методические рекомендации по организации изучения дисциплины «Моделирование систем защиты информации»

Методически обосновано изучать дисциплину в аудитории на лекциях, семинарских и самостоятельных занятиях.

Проведение лабораторных работ и практических занятий по курсу не предусмотрено.

Целесообразно для увеличения времени проработки важных тем предусмотреть рассмотрение отдельных вопросов в форме дискуссий и диспутов, на конференциях. Кроме того, необходимо предусмотреть дополнительные консультации по сложным темам.

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 самостоятельной подготовке.

При неаттестации хотя бы по одному из разделов, студент не допускается к зачету.

Автор(ы):

Гавдан Григорий Петрович

Рецензент(ы):

Горбатов В.С.