Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В 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	16	16		44	0	3
Итого	3	108	32	16	16	0	44	0	

АННОТАЦИЯ

Целью освоения учебной дисциплины является формирование компетенций по основным разделам теоретических и практических основ проектирования подсистем антивирусной защиты компьютерных систем с использованием методов искусственного интеллекта.

Основными задачами дисциплины являются:

• Ознакомление с особенностями работы и проектирования современных систем информационной безопасности, реализующих методы искусственного интеллекта.

• Изучение особенностей практического применения средств антивирусной защиты и ее актуализации с использованием искусственного интеллекта.

• Изучение технологий обнаружения вирусов в современных системах антивирусной защиты с использованием методов искусственного интеллекта.

• Изучение методов построения решающих правил в современных системах информационной безопасности с использованием методов искусственного интеллекта.

• Изучение методов искусственного интеллекта и их применения в современных системах информационной безопасности.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является формирование компетенций поосновным разделам теоретических и практических основ проектирования подсистем антивирусной защиты компьютерных систем с использованием методов искусственного интеллекта.

Основными задачами дисциплины являются:

• Ознакомление с особенностями работы и проектирования современных систем информационной безопасности, реализующих методы искусственного интеллекта.

• Изучение особенностей практического применения средств антивирусной защиты и ее актуализации с использованием искусственного интеллекта.

• Изучение технологий обнаружения вирусов в современных системах антивирусной защиты с использованием методов искусственного интеллекта.

• Изучение методов построения решающих правил в современных системах информационной безопасности с использованием методов искусственного интеллекта.

• Изучение методов искусственного интеллекта и их применения в современных системах информационной безопасности

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

дисциплина специализации

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
проектный			
разработка проектных решений по обеспечению информационной безопасности	информационные ресурсы	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики 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).
разработка проектных решений по обеспечению информационной безопасности	информационные ресурсы	ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032	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	Первый раздел	1-8	16/8/8		25	КИ-8	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2,

							В-ПК-2
2	Второй раздел	9-16	16/8/8		25	КИ-16	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2
	Итого за 3 Семестр		32/16/16		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

* – 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	32	16	16
1-8	**Первый раздел**	16	8	8
	Искусственный интеллект. Системы распознавания образов, их обучение и применение. -Искусственный интеллект и системы распознавания вокруг нас: в технической и медицинской диагностике, в экономике, управлении; проблема формализации при постановке задачи распознавания и машинного обучения; - общая структура системы распознавания: рецепторы, классификаторы, эффекторы; - основные классы задач распознавания, терминология: объекты, образы, классы и кластеры; - обучение и самообучение систем распознавания; - эффективность распознавания и ее оценка; - особенности применения систем распознавания в задачах диагностики и управления; -современные системы виртуальной и дополненной реальности; - машинное обучение и самообучение в системах виртуальной и дополненной реальности; -поиск и анализ актуальной информации о современных	Всего аудиторных часов 4 Онлайн 4	2 0	2 0

	системах распознавания образов и их использовании в задачах информационной безопасности.			
	Системы искусственного интеллекта. Информативные признаки и решающие правила. - Количественные, качественные и классификационные признаки и оценка их информативности; - Метрики Фишера и Шеннона; - Построение информативного признакового пространства; - Метод корреляционных плеяд; - Особенности оценки бинарных и качественных признаков; - Расстояния между объектами и классами; - Метрики Евклида, Шеннона, Минковского, Махаланобиса; - Расстояния ближних соседей, дальних соседей, центров классов; - Решающие правила и их классификация; - Параметрические и непараметрические методы; - Дискриминантный анализ; - Метод k-ближайших соседей; - Статистические методы распознавания; - Разработка сложных систем и деревьев решений; - Метод последовательной дихотомии; - Деревья решений и их оптимизация; - Методы поиска; - Качество распознавания и его оценка; - Обучающая и проверяющая выборки; - Вероятностные и экономические методы оценки	Всего аудиторных часов		
		4	2	2
		Онлайн		
		4	0	0
	Системы искусственного интеллекта. Обучение «без учителя» и кластеризация. - Обучение «без учителя» и кластеризация; - Понятия «кластер», «класс», «объект», «вектор признаков»; - Кластерный анализ и его применение в задачах обучения «без учителя» и GRID-технологиях: - Методы решения и эвристические процедуры; - Метод последовательных слияний; -Процедура Дубиссона; - Кривая Торндейка и оценка вероятного числа кластеров; - Кластеры-цепочки и их определение; - Применение перспективных методов кластерного анализа при разработке современных GRIDсистем.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		4	0	0
	Информационная безопасность и антивирусная защита. Вирусы и их классификация. - Проблема защиты программ и данных; -Информационная и кибербезопасность; -Проблема криминализации информационного пространства; - Вирусные атаки: потенциальные угрозы и методы защиты; - Решение задач антивирусной защиты на мировом уровне; - Применение перспективных методов исследования и	Всего аудиторных часов		
		4	2	2
		Онлайн		
		4	0	0

	решения профессиональных задач при разработке программ антивирусной защиты в государственных и коммерческих предприятиях России. - Вредоносные программы: компьютерные вирусы, черви, трояны и пр.; - Загрузочные и файловые вирусы; - Макровирусы и скрипт-вирусы; - Шифрование и метаморфизм.; - Черви: сетевые, почтовые, IM, IRC, P2P; - Трояны: клавиатурные шпионы, похитители паролей, утилиты скрытого удаленного управления, анонимные прокси-сервера, утилиты дозвона, логические бомбы, модификаторы настроек браузера; - Условно опасные программы: Riskware, Рекламные утилиты (adware), Pornware, злые шутки. - Российские базы данных вирусов и зарегистрированных инцидентов и организационно-правовые основы их использования в системах антивирусной защиты российских государственных организаций и коммерческих предприятий.			
9-16	**Второй раздел**	16	8	8
	Признаки присутствия на компьютере вредоносных программ и методы защиты от них. - Общие сведения и виды проявлений: явные, косвенные и скрытые; - Изменение настроек браузера; - Всплывающие сообщения; - Несанкционированное обращение к Интернет; - Блокирование антивируса; - Блокирование антивирусных сайтов; - Сбои в системе или в работе других программ; - Почтовые уведомления; - Скрытые проявления: наличие в памяти подозрительных процессов; наличие на компьютере подозрительных файлов; наличие подозрительных ключей в системном реестре Windows; подозрительная сетевая активность; - Применение методов искусственного интеллекта; - Где искать: процессы, автозапуск, системный реестр Windows, конфигурационные файлы, сетевая активность; - Методы обнаружения вредоносных программ и защиты от них; - Организационные методы (правила поведения, политика безопасности); - Технические методы (брэндмауэры, средства борьбы со спамом, закладки и пр.); - Черные и белые списки адресов; - Базы данных образцов спама; - Самообучение; - Анализ служебных заголовков; - Применение методов искусственного интеллекта;	Всего аудиторных часов 4 Онлайн 4	2 0	2 0

	- Поиск и анализ актуальной информации о современных признаках присутствия на компьютере вредоносных программ; - Проектирование программ обнаружения признаков присутствия вредоносных программ с использованием методов искусственного интеллекта.			
	Основы работы антивирусных программ. Применение методов распознавания образов. - Сигнатурные методы и эвристические методы.; -Сигнатурный анализ; - Эвристики; - Поиск вируса, похожего на известные: вероятность ошибочно определить наличие в файле вируса, невозможность лечения, низкая эффективность; - Поиск вируса, выполняющего подозрительные действия: удаление файла, запись в файл, запись в определенные области системного реестра, открытие порта на прослушивание, перехват данных вводимых с клавиатуры, рассылка писем; - Проблемы: ложные срабатывания, невозможность лечения, невысокая эффективность; - Базовые модули антивирусного ПО: модуль обновления, модуль планирования, модуль управления; - Функционал блока управления: Поддержка удаленного управления и настройки; - - Защита настроек от изменений, карантин; - Тестирование работы антивируса. -Применение перспективных методов при разработке современных антивирусных программ и систем информационной безопасности на базе методов искусственного интеллекта; -Проектирование базовых модулей антивирусного ПО.	Всего аудиторных часов 4 Онлайн 4	2 0	2 0
	Современные методы защиты от вирусов на базе методов искусственного интеллекта. - Методы, основанные на анализе содержимого файлов (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд; -Методы, основанные на отслеживании поведения программ при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции; -Методы регламентации порядка работы с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности. Один из наиболее распространенных методов этой группы состоит в том, что в системе (компьютере или	Всего аудиторных часов 4 Онлайн 4	2 0	2 0

	корпоративной сети) выполняются только те программы, запись о которых присутствует в списке программ, разрешенных к выполнению в данной системе. Этот список формируется администратором сети из проверенного программного обеспечения; -Наиболее популярные антивирусные программы и их особенности. McAfee, Norton, Panda, Avira, Bitdefender, Bullguard, Heimdal. Антивирус Касперского; -Применение методов искусственного интеллекта в наиболее популярных антивирусных программах в современных корпоративных системах киберзащиты.			
	Антивирусная защита домашнего компьютера и компьютерной сети с использованием методов искусственного интеллекта. -Антивирусное программное обеспечение; - Программы для защиты от несанкционированного доступа и сетевых хакерских атак; - Фильтры нежелательной корреспонденции; - Проверка в режиме реального времени; - Проверка по требованию; - Поддержание актуальности антивирусных баз; - Фильтрация нежелательных электронных сообщений; - Персональная антиспамовая программа; - Применение методов искусственного интеллекта в рассмотренных программах; - Применение перспективных методов при разработке антивирусных программ; - Проектирование антивирусного ПО для защиты домашнего компьютера на базе методов искусственного интеллекта; -Основы построения локальной компьютерной сети; - Рабочие станции и сетевые серверы, почтовые серверы и шлюзы; - Уровни антивирусной защиты: уровень защиты рабочих станций и сетевых серверов, уровень защиты почтовых серверов, уровень защиты шлюзов; - Централизованное управление антивирусной защитой; - Компоненты системы удаленного централизованного управления: клиентская антивирусная программа, сервер администрирования, агент администрирования, консоль администрирования; - Организация сбора статистики в системе антивирусной защиты и использование этой информации в интеллектуальных системах информационной безопасности; - Червь Caribe - вредоносная программа для мобильных телефонов; - Антивирусы для мобильных устройств; - Политики обеспечения информационной безопасности при работе с мобильными устройствами.	Всего аудиторных часов 4 Онлайн 4	2 0	2 0

	Политика «нулевого доверия»; -Разработка организационных методов реализации политики безопасности предприятия при проектировании системы антивирусной защиты для удаленных рабочих мест; -Организация и управление коллективной разработкой системы антивирусной защиты корпоративной сети предприятия, включающей удаленные рабочие места; - Применение методов искусственного интеллекта.			

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 ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	3 Семестр
	Л/Р 1 машинное обучение и самообучение в системах виртуальной и дополненной реальности
	Л/Р 2 Расстояния ближних соседей, дальних соседей, центров классов
	Л/Р 3 Самообучение
	Л/Р 4 Методы, основанные на анализе содержимого файлов

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии сочетают в себе совокупность методов и средств для реализации определенного содержания обучения и воспитания в рамках дисциплины, влючают решение дидактических и воспитательных задач, формируя основные понятия дисциплины, технологии проведения занятиий, усвоения новых знаний, технологии повторения и контроля материала, самостоятельной работы, современные компьютерные технологии.

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-1	З-ПК-1	З, КИ-8, КИ-16
	У-ПК-1	З, КИ-8, КИ-16
	В-ПК-1	З, КИ-8, 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-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:

<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</td></tr>
</table>

			студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом лекций и семинарских занятий, графиком контроля знаний.

Успешное освоение дисциплины требует от студентов посещения лекций, активной работы во время семинарских занятий, выполнения всех домашних заданий, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки.

При необходимости в конце лекции преподаватель оставляет время для того, чтобы студенты имели возможность задать вопросы по изучаемому материалу.

Лекции нацелены на освещение основополагающих положений теории алгоритмов и теории функций алгебры логики, наиболее трудных вопросов, как правило, связанных с доказательством необходимых утверждений и теорем, призваны способствовать формированию

навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам, а также для выполнения домашних заданий, которые выдаются после каждого семинара.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе лекций, аудиторных практических занятий, лабораторных и самостоятельных занятий.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов. Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и посвящены рассмотрению практических примеров и конкретизации материала, введенного на лекции. В лекционном курсе главное место отводится общетеоретическим проблемам.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в отечественных и зарубежных научно-практических публикациях;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечении по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и

средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и работе на семинарских занятиях.

Автор(ы):

Запечников Сергей Владимирович, д.т.н., доцент