Федеральное государственное бюджетное образовательное
учреждение высшего образования
Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики

УТВЕРЖДАЮ
декан факультета вычислительной
математики и кибернетики
_____/**И.А. Соколов /**
«20» 12 _____**2023 г.**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины:

Технологические угрозы и системы обеспечения кибербезопасности

Уровень высшего образования:

бакалавриат, магистратура, специалитет

Направление подготовки / специальность:

Направленность (профиль):

Форма обучения:

Очная с использованием дистанционных образовательных технологий

Москва 2023

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки программ бакалавриата, магистратуры, специалитета.

1. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО:

Является дисциплиной по выбору, избираемой в обязательном порядке.

2. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ:

Курс предназначен для студентов, которые планируют управлять безопасностью информационных система в коммерческих и государственных организациях. В рамках курса формулируются основные задачи подразделения информационной безопасности (ИБ), роль службы ИБ в общей организационной структуре, приводится описание основных видов угроз и доменов ИБ, покрытие которых необходимо для обеспечения защищенности данных и непрерывности процессов. Особое внимание уделяется таким ключевым понятиям как уязвимость ПО, типологии внешних и внутренних угроз ИБ, специфика обеспечения сетевой безопасности, понятия таргетированных атак и методов противодействия им. По окончании курса студенты получат представления о подходах к обоснованию инвестиций в ИБ, о возможностях и ограничениях применения внешних сервисов ИБ, о влиянии нормативного регулирования на системы и процессы ИБ в организации. Общая цель, которую призван достичь курс заключается в повышении уровня готовности выпускника к реальным задачам, стоящим перед службами ИБ в настоящее время, лучше ориентироваться в ландшафте актуальных угроз и понимать спектр основных подсистем обеспечения ИБ, механизмы их интегрированного использования, тенденции развития технологий обнаружения угроз ИБ и реагирования на них.

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ):

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	**Индикатор (показатель) достижения компетенции**	**Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций**
ОПК-5. Способен свободно ориентироваться в ландшафте современных угроз, а также грамотно планировать управление ИБ в организации.	ОПК-4.1. – знать и понимать основные принципы ИБ и классы возникающих угроз. ОПК-4.2. - уметь оценивать степень защищённости информационной chts организации. ОПК-4.3. - иметь практический опыт планирования мероприятий для защиты информационной среды организации от внешних и внутренних угроз.	**Знать**: основные понятия ИБ, основные виды современных угроз, современные методы защиты от кибер угроз, требования и стандарты ИБ. **Уметь**: делать обоснованный выбор средств защиты от внешних и внутренних угроз. **Иметь опыт**: планирования мероприятий для защиты информационной среды организации от внешних и внутренних угроз.

4. Объем дисциплины (модуля) составляет 24 академических часа, отведенных на контактную работу обучающихся с преподавателем. Форма отчетности – зачет.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДЫ УЧЕБНЫХ ЗАНЯТИЙ

5.1. Структура дисциплины (модуля) по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий (в строгом соответствии с учебным планом)

Наименование разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	Номинальные трудозатраты обучающегося			Всего академических часов	Форма текущего контроля успеваемости* (наименование)
	Контактная работа Виды контактной работы, академические часы		Самостоятельная работа обучающегося академические часы		
	Занятия лекционного типа	Занятия семинарского типа			
Тема 1. Введение в ИБ корпоративной среды.	2	0		2	
Тема 2. Внешние и внутренние угрозы ИБ и уязвимости. Обоснование инвестиций в ИБ.	2	0		2	
Тема 3. Сетевая безопасность.	2	0		2	
Тема 4. Введение в угрозы для конечных точек.	2	0		2	Колок-виум
Тема 5. Таргетированные атаки и сложные угрозы ИБ. Информация об угрозах (Cyber Threat Intelligence).	4	0		4	Колок-виум
Тема 6. Назначение, эволюция и сценарии использования SIEM. Основы практики реагирования на инциденты ИБ.	2	0		2	
Тема 7. Специфика оказания внешних сервисов в ИБ. XDR-платформа как инструмента корпоративного центра ИБ. Системы повышения осведомленности.	2	0		2	Колок-виум
Тема 8. Введение в корпоративные системы идентификации, ZeroTrust концепция. Модель контроля доступа к сети NAC. Защита облачных и контейнерных сред.	4	0		4	Колок-виум
Тема 9. Безопасность индустриальной среды. Защита Критической Инфраструктуры, ГОССОПКА. Понятие регуляторного соответствия в международной практике.	2	0		2	
Тема 10. Особенности применения средств ИИ в области информационной безопасности.	2	0		2	Колок-виум
Промежуточная аттестация (зачет)					зачет
Итого	24	0		24	—

5.2. Содержание разделов (тем) дисциплины

№ п/п	Наименование разделов (тем) дисциплины	Содержание разделов (тем) дисциплин
1.	Тема 1. Введение в ИБ корпоративной среды.	Понятие информационной безопасности (ИБ) корпоративной среды, основные принципы, проблемы и области знаний. Ролевая модель для обеспечения ИБ, понятие процессов и политик ИБ, роль службы ИБ в системе принятия решений в организации. Понятие риска ИБ, модели угроз, понятие нарушителя ИБ, типология

		кибер преступников. Основные виды технологических угроз для корпоративной среды, последствия и формы ущерба. Основные классы подсистем обеспечения ИБ, предназначение и ключевые возможности.
2.	Тема 2. Внешние и внутренние угрозы ИБ и уязвимости. Обоснование инвестиций в ИБ.	Понятие внутренних угроз, системы Data Leakage Protection (DLP), основные технологии обнаружения утечек. Понятие уязвимости информационной системы, понятие «уязвимости нулевого дня», примеры атак с использованием уязвимостей, формат описания уязвимостей, основные источники информации об уязвимостях. Системы обнаружения известных уязвимостей, проблемы управления программными обновлениями (patching), понятие слабой конфигурации (weak configuration) и практики повышения защищенности (system hardening). Понятие оценки защищенности корпоративной среды, сервисы тестирование на проникновения (Penetration test), концепция Ethical Hacking и поиска уязвимостей за вознаграждение (bug bounty). Обоснование инвестиций в информационную безопасность.
3.	Тема 3. Сетевая безопасность.	Понятие и основные подсистемы обеспечения сетевой информационной безопасности, назначение и ключевой функционал межсетевого экрана, NGFW, NTA, обеспечение сетевой безопасности в условиях программно-определяемой инфраструктуры. Назначение безопасности интернет-соединений (web security), роль проксирования, ключевые возможности решений классов UTM и SWG. Понятие и назначение систем безопасности почтовых коммуникаций (mail-security), основные виды архитектур, борьба со СПАМом. Понятие DDoS, типы и эволюция технологий проведения атак на отказ в обслуживании, вовлечение устройств класса IoT и сетевых решений в инфраструктуру атаки, кейс MIRAI, подходы к обеспечению защиты от DDoS, понятие «центра очистки траффика», понятие и основные сценарии использования WAF (web application firewall).
4.	Тема 4. Введение в угрозы для конечных точек.	Понятие вредоносного программного обеспечения (ЗПО), его виды, основные техники и сценарии проникновения, эволюционное развитие. Базовый функционал и архитектура система защиты рабочего места (EPP, End Point Protection) в корпоративной среде, понятие обнаружения ВПО, сигнатур, использование поведенческого и корреляционного анализа. Особенности управления системой EPP в организации, в изолированной и облачной среде, особенности защиты почты и мобильных устройств. Ограничения применимости и эффективности классических решений EPP, понятие сложных угроз, таргетированных атак, APT, анатомия и фазы.
5.	Тема 5. Таргетированные атаки и сложные угрозы ИБ. Информация об угрозах (Cyber Threat Intelligence).	Примеры обнаруженных и описанных таргетированных атак и APT. Методы обнаружения сложных атак, MITRE ATT&CK ® матрица, понятие систем класса EDR (Endpoint Detection and Response). Виды Cyber Threat Intelligence (CTI), архитектурные модели использования в корпоративной среде, понятие TIP (Threat Intelligence Platform).
6.	Тема 6. Назначение, эволюция и сценарии использования SIEM. Основы практики	Понятие SIEM (security information event management) платформы как ключевой подсистемы в обеспечении ИБ крупной организации, базовая архитектура, основной функционал и сценарии использования. Расследование инцидента (Incident Response)

	реагирования на инциденты ИБ.	нарушения ИБ, необходимый инструментарий и навыки службы ИБ, способы обеспечения постоянного контроля ИБ корпоративной среды, внешние сервисы мониторинга, проблемы выбора подхода. Понятие внешнего сервис провайдера в ИБ (MSSP, Managed Security Service Provider), сервисный каталог, понятие SLA, зоны ответственности и лучшие практики привлечения поставщиков сервисов ИБ.
7.	Тема 7. Специфика оказания внешних сервисов в ИБ. XDR-платформа как инструмента корпоративного центра ИБ. Системы повышения осведомленности.	Понятие и назначение SOC (Security Operation Center), ключевые процессы, шаги внедрения, архитектурные подходы, “modern SOC”. XDR (eXtended Detection and Response) как эволюционное объединение функций обеспечения корпоративной ИБ, основы SOAR систем. Программа повышения осведомленности сотрудников в вопросах ИБ.
8.	Тема 8. Введение в корпоративные системы идентификации, ZeroTrust концепция. Модель контроля доступа к сети NAC. Защита облачных и контейнерных сред.	Понятие системы идентификации пользователей в сети, учетной записи, подходы к identity management, понятие Single Sign On (SSO). Идея автоматизации контроля доступа к сети (NAC), концепция Zero Trust, принципы и необходимые подсистемы ИБ. Специфика ИБ для виртуальных, облачных и контейнерных сред, угрозы, ключевой функционал решений, понятие DevOps и DevSecOps.
9.	Тема 9. Безопасность индустриальной среды. Защита Критической Инфраструктуры, ГОССОПКА. Понятие регуляторного соответствия в международной практике.	Информационная безопасность индустриальной среды, особенности и применяемые подсистемы ИБ. Понятие Критической Информационной Инфраструктуры (КИИ), государственная система обеспечения безопасности КИИ и необходимые средства обеспечения ИБ, понятие и виды CERT. Важность соответствие регуляторным требованиями (compliance) и стандартам ИБ, примеры требований, формальный подход к соответствию.
10.	Тема 10. Особенности применения средств ИИ в области информационной безопасности.	Влияние инструментов ML и элементов ИИ на кибер-угрозы и информационную безопасность.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ФОС, ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ) ДЛЯ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ).

Список вопросов к зачету

1. Внешние и внутренние угрозы ИБ и уязвимости.
2. Понятие и основные подсистемы обеспечения сетевой информационной безопасности.
3. Понятие вредоносного программного обеспечения (ЗПО), его виды, основные техники и сценарии проникновения, эволюционное развитие.
4. Таргетированные атаки и сложные угрозы ИБ. Информация об угрозах (Cyber Threat Intelligence).
5. Понятие SIEM (security information event management) платформы как ключевой подсистемы в обеспечении ИБ крупной организации, базовая архитектура, основной функционал и сценарии использования..
6. Понятие и назначение SOC (Security Operation Center), ключевые процессы, шаги внедрения, архитектурные подходы.
7. Информационная безопасность индустриальной среды, особенности и применяемые подсистемы ИБ.

Методические материалы для проведения процедур оценивания результатов обучения

Особенности организации процесса обучения

Для эффективного освоения курса рекомендуется перед каждым занятие привести в порядок конспекты лекций. После каждого занятия рекомендуется найти и прочитать дополнительную литературу по теме лекции и прочитать свои конспекты.

Система контроля и оценивания

За каждую домашнюю выставляются баллы (максимум 40 баллов). Пусть M – максимальное число баллов, которое может набрать студент. В конце семестра баллы конвертируются в оценку O1 следующим образом:

меньше M/2 баллов: O1=2;

больше или равно M/2 баллов, но меньше 2M/3: O1=3;

больше или равно 2M/3 баллов, но меньше 5M/6: O1=4;

больше или равно 5M/6 баллов: O1=5.

На экзамене оценка O1 является стартовой. Окончательная оценка определяется исходя из оценки устного ответа студента, при этом она не может отличаться от стартовой оценки более чем на 1 балл.

Структура и график контрольных мероприятий

Устная сдача домашних заданий в конце каждой недели, устный экзамен в конце семестра.

7. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ:

7.1. Перечень основной и дополнительной литературы

Основная литература

1. А.П.Курило [и др.] Обеспечение информационной безопасности бизнеса, БДЦ-пресс, 2005.
2. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems 3rd Edition
3. Qing Li, Gregory Clark, Security Intelligence: A Practitioner's guide to solving enterprise security challenges, John Wiley & Sons, 2015
4. K. Knerler, I.Parker, C.Zimmerman (MITRE), 11 Strategies of a world-class cybersecurity operations center, 2022, https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf
5. Eric Cole, Advanced Persistent Threat – Understanding the danger and how to protect your organization, Syngress, 2013
6. Evan Gilman, Doug Barth, Zero trust networks – Building secure systems in untrusted networks, O'reilly, 2017
7. Andrew A. Bochman, Sarah Freeman - Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE), 2021
8. Басыня Е.А. Системное администрирование и информационная безопасность, Издательство НГТУ 2018
9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях, Издательство ДМК Пресс, 2013
10. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных систем предприятий, Издательство ВШЭ, 2012
11. Терри Оглтри Firewalls. Практическое применение межсетевых экранов, ДМК Пресс, 2017
12. Роджер Граймс Как противостоять хакерским атакам. Уроки экспертов по информационной безопасности. Издательство Бомбора, 2023
13. Касперский Е.В. Компьютерное зловредство, Издательство Питер, 2007
14. Скулкин О. Шифровальщики: Как реагировать на атаки с использованием программ-вымогателей. Альпина PRO, 2023
15. С.А.Петренко, В.А. Курбатов Политики информационной безопасности, ДМК Пресс 2015
16. MITRE ATT&CK® https://attack.mitre.org/

Дополнительная литература

17. Howard Chivers, “Malware and Attack Technologies Knowledge Area Issue 1.0”, [Online]. Available: https://www.cybok.org/media/downloads/Malware__Attack_Technology_issue_1.0.pdf.
18. M. Sikorski and A. Honig, Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software. No Starch Press, 2012.

7.2.Перечень лицензионного программного обеспечения, в том числе отечественного производства

При реализации дисциплины может быть использовано следующее программное обеспечение:

- Операционная система Windows
- Операционная система Debian Linux
- Программное обеспечение для подготовки слайдов лекций MS PowerPoint, MS Word
- Программное обеспечение для создания и просмотра pdf-документов Adobe Reader
- Издательская система LaTeX
- Язык программирования Python и среда разработки Jupiter Notebook (вместе с библиотеками numpy, scikit-learn, pandas)
- Язык программирования R и среда разработки R Studio
- Файловый архиватор 7z. Свободно-распространяемое ПО
- Браузеры Google Chrome, Mozilla Firefox. Свободно-распространяемое ПО
- Офисный пакет LibreOffice. Свободно-распространяемое ПО
- Visual Studio Community Интегрированная среда разработки ПО. Свободно-распространяемое ПО
- PyCharm Community Интегрированная среда разработки ПО. Свободно-распространяемое ПО
- Anaconda Интегрированная среда разработки ПО. Свободно-распространяемое ПО

7.3.Перечень профессиональных баз данных и информационных справочных систем

1. http://www.edu.ru – портал Министерства образования и науки РФ
2. http://www.ict.edu.ru – система федеральных образовательных порталов «ИКТ в образовании»
3. http://www.openet.ru - Российский портал открытого образования
4. http://www.mon.gov.ru - Министерство образования и науки Российской Федерации
5. http://www.fasi.gov.ru - Федеральное агентство по науке и инновациям

7.4.Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц.
URL: http://www.mathnet.ru

2. Университетская библиотека Online [Электронный ресурс] : электронная библиотечная система / ООО "Директ-Медиа" . - М. : [б. и.], 2001. - Загл. с титул. экрана. - Б. ц. URL: www.biblioclub.ru

3. Универсальные базы данных EastView [Электронный ресурс] : информационный ресурс / EastViewInformationServices. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. ц.
URL: www.ebiblioteka.ru

4. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] : информационный портал / ООО "РУНЭБ" ; Санкт-Петербургский государственный университет. - М. : [б. и.], 2005. - Загл. с титул. экрана. - Б. ц.

URL: www.eLibrary.ru

7.5.Описание материально-технического обеспечения.

Образовательная организация, ответственная за реализацию данной Программы, располагает соответствующей материально-технической базой, включая современную вычислительную

технику, объединенную в локальную вычислительную сеть, имеющую выход в Интернет. Используются специализированные компьютерные классы, оснащенные современным оборудованием. Материальная база соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов занятий (лекционных, практических, семинарских, лабораторных, дисциплинарной и междисциплинарной подготовки) и научно-исследовательской работы обучающихся, предусмотренных учебным планом.

8. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

8.1. Формы и методы преподавания дисциплины

Используемые формы и методы обучения: лекции и лабораторные работы, самостоятельная работа студентов.

В процессе преподавания дисциплины преподаватель использует как классические формы и методы обучения (лекции и практические занятия), так и активные методы обучения.

При проведении лекционных занятий преподаватель использует аудиовизуальные, компьютерные и мультимедийные средства обучения, а также демонстрационные и наглядно-иллюстрационные (в том числе раздаточные) материалы.

Семинарские (практические) занятия по данной дисциплине проводятся с использованием компьютерного и мультимедийного оборудования, при необходимости - с привлечением полезных Интернет-ресурсов и пакетов прикладных программ.

8.2. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить студентов с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

1) формулирует тему и цель занятия;

2) излагает основные теоретические положения;

3) с помощью мультимедийного оборудования и/или под запись дает определения основных понятий, расчетных формул;

4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;

5) в конце занятия дает вопросы для самостоятельного изучения.

Во время выполнения заданий в учебной аудитории студент может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных за-дач. Если какая-то часть задания остается не выполненной, студент может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

Для семинарских занятий

Подготовка к проведению занятий проводится регулярно. Организация преподавателем семинарских занятий должна удовлетворять следующим требования: количество занятий должно соответствовать учебному плану программы, содержание планов должно соответствовать программе, план занятий должен содержать перечень рассматриваемых вопросов.

Во время семинарских занятий используются словесные методы обучения, как беседа и дискуссия, что позволяет вовлекать в учебный процесс всех слушателей и стимулирует творческий потенциал обучающихся.

При подготовке семинарскому занятию преподавателю необходимо знать план его проведения, продумать формулировки и содержание учебных вопросов, выносимых на обсуждение.

В начале занятия преподаватель должен раскрыть теоретическую и практическую значимость темы занятия, определить порядок его проведения, время на обсуждение каждого учебного вопроса. В ходе занятия следует дать возможность выступить всем желающим и предложить выступить тем слушателям, которые проявляют пассивность.

Целесообразно, в ходе обсуждения учебных вопросов, задавать выступающим и аудитории дополнительные и уточняющие вопросы с целью выяснения их позиций по существу обсуждаемых проблем, а также поощрять выступление с места в виде кратких дополнений. На занятиях проводится отработка практических умений под контролем преподавателя

Для практических занятий

Подготовка преподавателя к проведению практического занятия начинается с изучения исходной документации и заканчивается оформлением плана проведения занятия.

На основе изучения исходной документации у преподавателя должно сложиться представление о целях и задачах практического занятия и о том объеме работ, который должен выполнить каждый обучающийся. Далее можно приступить к разработке содержания практического занятия. Для этого преподавателю (даже если он сам читает лекции по этому курсу) целесообразно вновь просмотреть содержание лекции с точки зрения предстоящего практического занятия. Необходимо выделить понятия, положения, закономерности, которые следует еще раз проиллюстрировать на конкретных задачах и упражнениях. Таким образом, производится отбор содержания, подлежащего усвоению.

Важнейшим элементом практического занятия является учебная задача (проблема), предлагаемая для решения. Преподаватель, подбирая примеры (задачи и логические задания) для практического занятия, должен представлять дидактическую цель: привитие каких навыков и умений применительно к каждой задаче установить, каких усилий от обучающихся она потребует, в чем должно проявиться творчество студентов при решении данной задачи.

Преподаватель должен проводить занятие так, чтобы на всем его протяжении студенты были заняты напряженной творческой работой, поисками правильных и точных решений, чтобы каждый получил возможность раскрыться, проявить свои способности. Поэтому при планировании занятия и разработке индивидуальных заданий преподавателю важно учитывать подготовку и интересы каждого студента. Педагог в этом случае выступает в роли консультанта, способного вовремя оказать необходимую помощь, не подавляя самостоятельности и инициативы студента.

8.3. Методические рекомендации студентам по организации самостоятельной работы.

Приступая к изучению новой учебной дисциплины, студенты должны ознакомиться с учебной программой, учебной, научной и методической литературой, имеющейся в библиотеке университета, встретиться с преподавателем, ведущим дисциплину, получить в библиотеке рекомендованные учебники и учебно-методические пособия, осуществить запись на соответствующий курс в среде электронного обучения университета.

Глубина усвоения дисциплины зависит от активной и систематической работы студента на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

На лекциях важно сосредоточить внимание на ее содержании. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине. Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки,

раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы. Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности студентов.

Методические указания для обучающихся по подготовке к семинарским занятиям

Для того чтобы семинарские занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на семинарских занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач.

При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

При подготовке к семинарским занятиям следует использовать основную литературу из представленного списка, а также руководствоваться приведенными указаниями и рекомендациями. Для наиболее глубокого освоения дисциплины рекомендуется изучать литературу, обозначенную как «дополнительная» в представленном списке.

Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий по данной дисциплине является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации: изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т. д.; при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа студента под управлением преподавателя. На них пополняются теоретические знания студентов, их умение творчески мыслить, анализировать, обобщать

изученный материал, проверяется отношение студентов к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы. После подведения итогов занятия студент обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

Методические указания для самостоятельной работы обучающихся

Прочное усвоение и долговременное закрепление учебного материала невозможно без продуманной самостоятельной работы. Такая работа требует от студента значительных усилий, творчества и высокой организованности. В ходе самостоятельной работы студенты выполняют следующие задачи: дорабатывают лекции, изучают рекомендованную литературу, готовятся к практическим занятиям, к коллоквиуму, контрольным работам по отдельным темам дисциплины. При этом эффективность учебной деятельности студента во многом зависит от того, как он распорядился выделенным для самостоятельной работы бюджетом времени.

Результатом самостоятельной работы является прочное усвоение материалов по предмету согласно программы дисциплины. В итоге этой работы формируются профессиональные умения и компетенции, развивается творческий подход к решению возникших в ходе учебной деятельности проблемных задач, появляется самостоятельности мышления.

Решение задач

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи).

Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом.

Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты.

Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

Задача — это цель, заданная в определенных условиях, решение задачи — процесс достижения поставленной цели, поиск необходимых для этого средств.

Алгоритм решения задач:

1. Внимательно прочитайте условие задания и уясните основной вопрос, представьте процессы и явления, описанные в условии.

2. Повторно прочтите условие для того, чтобы чётко представить основной вопрос, проблему, цель решения, заданные величины, опираясь на которые можно вести поиски решения.

3. Произведите краткую запись условия задания.

4. Если необходимо составьте таблицу, схему, рисунок или чертёж.

5. Определите метод решения задания, составьте план решения.

6. Запишите основные понятия, формулы, описывающие процессы, предложенные заданной системой.

7. Найдите решение в общем виде, выразив искомые величины через заданные.

9. Проверьте правильность решения задания.

10. Произведите оценку реальности полученного решения.

11. Запишите ответ.