Балаковский инженерно-технологический институт – филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»

Факультет атомной энергетики и технологий
Кафедра «Информационные системы и технологии»

РАБОЧАЯ ПРОГРАММА

по дисциплине «Информационная безопасность»

Направления подготовки
«09.03.02 Информационные системы и технологии»

Основная профессиональная образовательная программа
«Информационные системы и технологии»

Квалификация выпускника
Бакалавр

Форма обучения
Очная

Балаково

Цель освоения учебной дисциплины

Цель освоения дисциплины в области обучения, воспитания, развития, соотнесенные с общими целями ООП ВО являются: формирование психологической готовности к профессиональной деятельности по избранной профессии, формирование представления об основах информационной безопасности, принципов создания, модификации и сопровождения информационных (автоматизированных) систем с учётом норм и требований к ИБ; изучение современных угроз информационной безопасности и овладение комплексом мер, реализующих защиту информации на различных уровнях.

Место учебной дисциплины в структуре ООП ВО

Необходимыми условиями для освоения дисциплины являются знания, умения и практические навыки по предшествующим дисциплинам и практикам:

- Информатика;
- Информационные технологии;
- Управление информационными ресурсами ;
- Протоколы и интерфейсы информационных систем ;

Знания, умения и практические навыки, полученные при освоении дисциплины, необходимы при изучении следующих дисциплин и прохождения практик:

- Инфокоммуникационные системы и сети;
- Государственная итоговая аттестация.

Компетенции обучающегося, формируемые в результате освоения дисциплины

В процессе освоения данной дисциплины у студента формируются следующие компетенции:

общепрофессиональные

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	З-ОПК-3 – источники информации, необходимой для решения задач профессиональной деятельности; принципы обеспечения безопасности при работе с информационными системами У-ОПК-3 – осуществлять поиск необходимой информации для решения задач профессиональной деятельности на основе информационной и библиографической культуры В-ОПК-3 – методами поиска информации в локальных и глобальных сетях с соблюдением требований информационной безопасности
ОПК-5	Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	З-ОПК-5 – основы системного администрирования; архитектуру, устройство и функционирование информационных систем; основы современных операционных систем У-ОПК-5 – инсталлировать программное и аппаратное обеспечение; производить настройки параметров программного обеспечения В-ОПК-5 – методами установки и настройки программного и аппаратного обеспечения

Задачи воспитания, реализуемые в рамках освоения дисциплины

Направление/цели	Создание условий, обеспечивающих	Использование воспитательного потенциала учебной дисциплины	Вовлечение в разноплановую внеучебную деятельность
Профессиональное и трудовое воспитание	формирование психологической готовности к профессиональной деятельности по избранной профессии **(В15)**	Использование воспитательного потенциала дисциплин общепрофессионального модуля для: - формирования устойчивого интереса к профессиональной деятельности, потребности в достижении результата, понимания функциональных обязанностей и задач избранной профессиональной деятельности, чувства профессиональной ответственности через выполнение учебных, в том числе практических заданий, требующих строгого соблюдения правил техники безопасности и инструкций по работе с оборудованием в рамках лабораторного практикума.	1.Организация научно-практических конференций и встреч с ведущими специалистами предприятий города и ветеранами атомной отрасли. 2. Организация и проведение предметных олимпиад и участие в конкурсах профессионального мастерства. 3.Участие в ежегодных акциях студенческих строительных отрядов

Структура и содержание учебной дисциплины

Дисциплина изучается студентами в 7-ом семестре. Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 ак. часов.

Календарный план

№ Раздела	№ Темы	Наименование раздела (темы) дисциплины	Виды учебной деятельности (час.)					Аттестация раздела (форма)	Максимальный балл за раздел
			Всего	Лекции	Лабораторные	Практические	СРС		
1	**Основы информационной безопасности**								
	1	Общиепонятия информационной безопасности	20	4	-	4	12	КИ	25
	2	Угрозы информационной безопасности	22	6/2*	-	4	12		
	3	Направления обеспечения информационной безопасности	28	6/2	-	8	14		
2	**Информационная безопасность вычислительных систем сетей**								
	4	Криптографическая защита информации	28	4/2	-	10/10	14	КИ	25
	5	Анализ уязвимости информационных систем и оценка рисков	20	6/2	-	-	14		
	6	Безопасность информационных сетей	26	6/2	-	6	14		
Вид промежуточной аттестации			36					Э	50
Всего			**180**	**32/10**		**32/10**	**80**		**100**

Сокращенное наименование форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
КИ	Контроль итогов
Э	Экзамен

* - занятия в интерактивной форме

Содержание лекционного курса

Тема лекции. Вопросы, отрабатываемые на лекции	Всего часов	Учебно-методическое обеспечение
1	2	3
Общие понятия информационной безопасности. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение). Определение и цели информационной безопасности. Механизмы и принципы информационной безопасности. Общая проблема информационной безопасности информационных систем. Инструментарий информационной безопасности. Основные направления информационной безопасности. Категории информационной безопасности (конфиденциальность, целостность, доступность). Актуальность проблемы защиты информации. Общая постановка проблемы обеспечения информационной безопасности. Терминология. Задачи и принципы системы защиты информации. Программа информационной безопасности России и пути её реализации. Концептуальная модель информационной безопасности (ИБ). Основы государственной политики в области ИБ. Структура законодательства РФ в области защиты информации. Государственная политика РФ в области ИБ.	4	1-7
Угрозы информационной безопасности. Общая проблема информационной безопасности информационных систем. Понятие и определение «угрозы». Классификация угроз ИБ. Основные внешние и внутренние угрозы. Понятие «инсайдеры». Естественные и искусственные угрозы. Преднамеренные и непреднамеренные угрозы. Пути реализации угроз безопасности. Источники угроз. Спектр наиболее опасных угроз ИБ в РФ. Понятие уязвимость, угроза, атака. Разглашение, утечка и несанкционированный доступ (НСД). Причины, виды и каналы утечки информации. Технические и организационные каналы утечки информации. Наиболее распространённые угрозы ИБ в ИС. Описание модели гипотетического нарушителя.	6	1-7
Направления обеспечения информационной безопасности. Организационное обеспечение информационной безопасности. Классификация методов и средств защиты информации. Абстрактные модели защиты информации. Правовая зашита информации. Организационная (административная) защита данных. Проблемы и структура организационной защиты. Распространение объектно-ориентированного подхода на ИБ. О необходимости ООП к ИБ. Общая характеристика организационных методов защиты. Инженерно-техническая защита (ИТЗ) информации. Характеристика и основные задачи физических и аппаратных средств защиты. Программные средства защиты. Основные направления использования программ для обеспечения безопасности информации. Криптографические средства защиты. Комбинированные методы защиты.	6	1-7
Криптографическая защита информации. Математические и методические средства защиты. Основные определения	4	1-7

криптологии. Основные требования к современным методам шифрования. Классификация методов криптографического закрытия информации. Криптографические методы. Идентификация и аутентификация		
Анализ уязвимости информационных систем и оценка рисков. Защита информации от несанкционированного доступа. Уязвимость информационных систем. Классификация сетевых атак. Снифферы пакетов. IP-спуфинг. Отказ в обслуживании (Denial of Service - DoS). Парольные атаки. Атаки типа Man-in-the-Middle. Атаки на уровне приложений. Сетевая разведка. Злоупотребление доверием. Переадресация портов. Несанкционированный доступ. Безопасность операционных систем. Законодательный уровень и стандарты ИБ.	6	1-7
Безопасность информационных сетей. Протоколирование и аудит. Компьютерные вирусы, их свойства и классификация. Методы обнаружения и удаления компьютерных вирусов. Общие меры защиты информации от вирусов. Понятие атаки на систему информационной безопасности. Особенности локальных атак на систему информационной безопасности. Удаленные атаки на систему информационной безопасности. Межсетевые экраны и методы создания защищенных систем включающих межсетевые экраны. Виртуальные частные сети, их функции и назначение. Многоуровневая защита корпоративных сетей. Анализ системы защиты.	6	1-7

Перечень практических занятий

Тема практического занятия. Задания, вопросы, отрабатываемые на практическом занятии	Всего часов	Учебно-методическое обеспечение
1	2	3
Правовое обеспечение зашиты информации РФ	4	1-7
Безопасность операционных систем	4	1-7
Создание программного обеспечения парольной защиты и аутентификации	8	1-7
Моделирование процессов шифрования с помощью криптографического алгоритмов замены	4	1-7
Моделирование процессов шифрования, дешифрования с помощью криптографического алгоритма перестановок	6	1-7
Безопасная работа в компьютерных сетях	6	1-7

Перечень лабораторных работ

Лабораторные работы Учебным планом не предусмотрены.

Задания для самостоятельной работы студентов

Задания, вопросы, для самостоятельного изучения (задания)	Всего часов	Учебно-методическое обеспечение
1	2	3
Недочеты доктрины информационной безопасности. Примеры зарубежного законодательства в сфере информационной безопасности. Примеры систем защиты информации.	12	1-7
Классификация источников угроз. Спектр наиболее опасных угроз зарубежных стран.	12	1-7
Примеры реализации организационных методов защиты информации. Применение комбинированных методов защиты информации.	14	1-7

Обзор современных алгоритмов криптографии. Применение блочного шифрования в глобальных и локальных сетях.	14	1-7
Допущения в моделях оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Требования к защите, определяемые структурой автоматизированной системы обработки данных.	14	1-7
Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.	14	1-7

Расчетно-графическая работа

Расчетно-графическая работа Учебным планом не предусмотрена.

Курсовая работа

Курсовая работа Учебным планом не предусмотрена.

Курсовой проект

Курсовой проект Учебным планом не предусмотрен.

Образовательные технологии

При реализации учебного материала курса используются различные образовательные технологии, способствующие созданию атмосферы свободной и творческой дискуссии как между преподавателем и студентами, так и в студенческой группе. Целью при этом является выработка у студентов навыков и компетенций, позволяющих самостоятельно вести исследовательскую и научно-педагогическую работу.

Аудиторные занятия проводятся в виде лекций с использованием ПК и компьютерного проектора, практических занятий, с использованием ПК при проведении расчетов. Самостоятельная работа студентов проводится под руководством преподавателей, с оказанием консультаций и помощи при подготовке к контрольным работам, выполнении домашних заданий.

В рамках самостоятельной работы студенты изучают электронные образовательные курсы в онлайн формате.

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:

№ п/п	Наименование контролируемых разделов (темы)	Код и наименование индикатора достижения компетенций	Наименование оценочного средства
Входной контроль			
1	Входной контроль		Вопросы входного контроля (устно)
Аттестация разделов, текущий контроль успеваемости			
2	Основы информационной безопасности	З-ОПК-3, З-ОПК-5, У-ОПК-3, У-ОПК-5, В-ОПК-3, В-ОПК-5	Контроль итогов (в форме тестирования)
3	Информационная	З-ОПК-3, З-ОПК-5, У-ОПК-3,	Контроль итогов (в форме

	безопасность вычислительных систем сетей	У-ОПК-5, В-ОПК-3, В-ОПК-5	тестирования)
Промежуточная аттестация			
4	Экзамен	З-ОПК-3, З-ОПК-5, У-ОПК-3, У-ОПК-5, В-ОПК-3, В-ОПК-5	Вопросы к экзамену (письменно)

Входной контроль предназначен для выявления пробелов в знаниях студентов и готовности их к получению новых знаний. Оценочные средства для входного контроля представляют собой вопросы, которые задаются студентам в устной форме.

Перечень вопросов входного контроля

Вопросы входного контроля.

1) Сформулировать понятия информации и данных.
2) Описать пользователей информационной системы.
3) Дать определение предметной области, объекта, атрибута, структурная связи, концептуальной схемы.
4) Перечислить и описать этапы проектирования информационной системы.
5) Охарактеризовать программное обеспечение информационной системы.
6) Защита компьютерной информации от вредоносных программ

Текущий контроль – это непрерывно осуществляемый мониторинг уровня усвоения знаний и формирования умений и навыков в течение семестра. Текущий контроль знаний, умений и навыков студентов осуществляется в ходе учебных (аудиторных) занятий, проводимых по расписанию. Формами текущего контроля выступают опросы на практических занятиях, доклады и др.

Аттестация раздела по дисциплине проводится в форме контроля итогов в формате тестирования. Тест содержит от 10 вопросов. На выполнение задания отводится 30 минут. Тест – это форма контроля, направленная на проверку уровня освоения контролируемого теоретического и практического материала по дидактическим единицам дисциплины (терминологический аппарат, основные методы).

Примерный перечень тестовых заданий:

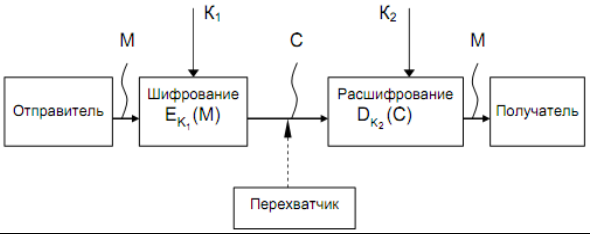
Тестовые задания 1. (КИ1)

1	Защита информации – это … 1) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры **2) комплекс мероприятий, направленных на обеспечение информационной безопасности** 3) актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
2	Согласно "Оранжевой книге", политика безопасности включает в себя следующие элементы: **1) метки безопасности** 2) периметр безопасности сертификаты безопасности
3	Степень доверия оценивается по следующим основным критериям а) политика безопасности 1) б, в, г б) уровень гарантированности **2) а, б**

	в) преобразование данных 3) а, в, г г) загрузка данных 4) а, г
4	Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней а) законодательного 1) а, в, г б) административного 2) а, б, в в) процедурного **3) а, б, в, г** г) программно-технического 4) б, г
5	Грани вредоносного ПО а) вредоносная функция 1) б, г б) алгоритм работы 2) а, б, в в) способ распространения 3) а, б, в, г г) внешнее представление **4) а, в, г**
6	Угрозы можно классифицировать по способу осуществления а) случайные 1) б, в, г б) преднамеренные 2) в, г в) действия природного 3) а, в, г г) техногенного характера **4) а, б, в, г**
7	Какой уровень детализации ИС изображен на рисунке ИС организации 1) уровень детализации 1 **2) уровень детализации 0** 3) уровень детализации 2 4) уровень детализации 3
8	Необходимость объектно-ориентированного подхода к информационной безопасности является следствием того, что: 1) это простой способ придать информационной безопасности научный вид 2) в информационной безопасности с самого начала фигурируют понятия объекта и субъекта **3) объектно-ориентированный подход - универсальное средство борьбы со сложностью современных информационных систем**
9	Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают: 1) средства выявления злоумышленной активности **2) средства контроля эффективности защиты информации** 3) средства обеспечения отказоустойчивости
10	Основными источниками внутренних отказов являются а) разрушение данных 1) а, б, в, г б) отступление (случайное или умышленное) от установленных правил эксплуатации 2) а, б, в в) ошибки при (пере)конфигурировании системы **3) в, г** г) отказы программного и аппаратного обеспечения 4) б, г

Тестовые задания 2. (КИ2)

1	Шифрование перестановкой заключается в том, что 1) шифруемый текст преобразуется по некоторому аналитическому правилу (формуле) 2) символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены 3) символы шифруемого текста складываются с символами некоторой случайной

	последовательности, именуемой гаммой шифра **4) символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста**
2	Перечислите шифры перестановки а) Система шифрования Цезаря — 1) в, г, д б) Шифрующие таблицы — 2) а, б, в, г, д в) Применение магических квадратов — **3) а, г, д** г) Шифрующие таблицы Трисемуса — 4) б, г д) Биграммный шифр Плейфейра
3	Какая схема криптосистемы изображена на рисунке 1) **ассимметричная** 2) симметричная 3) обобщенная 
4	К недостаткам системы Цезаря следует отнести следующие а) не маскируют частоты появления различных букв исходного открытого текста б) сохраняется алфавитный порядок в последовательности заменяющих букв в) шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифртексте. г) число возможных ключей К мало 1) в, г **2) а, б, в, г** 3) а, б, в 4) а, в
5	Зашифровать сообщение: «ВЫЛЕТАЕМ ПЯТОГО» с помощью шифрующей таблицы Трисемуса 1) ОИРМЕОС ЮВТАЬЛГО 2) ГНВЕП ЛТООА ДРНЕВ 3) **ПД КЗЫВЗ ЧШЛЫЙСЙ** 4) РПОТМ БЧМОР СОЫЬИ
6	Перечислите требования к шифрам, используемым для криптографической защиты информации а) простота процедур шифрования и расшифрования б) незначительная избыточность информации за счет шифрования в) нечувствительность к небольшим ошибкам шифрования г) достаточная криптостойкость (надежность закрытия данных) 1) а, в, г 2) а, в **3) а, б, в, г** 4) б, г
7	В число граней, позволяющих структурировать средства достижения информационной безопасности, входят: **1) административные меры** 2) меры обеспечения целостности 3) меры административного воздействия меры обеспечения доступности
8	Основной характеристикой шифра является 1) **криптостойкость** 2) ключ 3) мощность алгоритма
9	Что из перечисленного не относится к числу основных аспектов информационной безопасности: а) доступность б) целостность 1) **в** 2) в, г

	в) защита от копирования г) конфиденциальность систем	3) г 4) б
10	Политика безопасности строится на основе: 1) общих представлений об ИС организации 2) изучения политик родственных организаций 3) **анализа рисков**	

Критерии оценки тестовых заданий, устных опросов:

1. Полнота знаний теоретического контролируемого материала.
2. Количество правильных ответов.

Тестовое задание / опрос считается сданным, если студент правильно ответил на 60 процентов от общего числа вопросов.

Критерии оценивания	**Оценка**
Студент ответил на 90 % (и более) вопросов	Отлично
Студент ответил на 70-89 % вопросов	Хорошо
Студент ответил на 60-69 % вопросов	Удовлетворительно
Студент ответил менее чем на 59 % вопросов	Неудовлетворительно

Сумма баллов по разделам дисциплины складывается из оценок, полученных обучающимся в течение семестра по всем формам текущего контроля. Каждая форма контроля оценивается баллом в интервале от 0 до 10.

Промежуточная аттестация осуществляется в форме экзамена.

Перечень вопросов для подготовки к экзамену:

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Важность и сложность проблемы информационной безопасности.
4. Аспекты информационной безопасности.
5. Распространение объектно-ориентированного подхода на ИБ.
6. Основные понятия ООП в отношении к ИБ.
7. Уровни детализации ИС.
8. Компоненты и контейнеры.
9. Применение ООП к рассмотрению защищаемых систем.
10. Недостатки традиционного подхода к ИБ с объектной точки зрения.
11. Наиболее распространенные угрозы ИС. Основные понятия.
12. Классификация угроз.
13. Основные определения и критерии классификации угроз.
14. Вредоносное программное обеспечение. Грани вредоносного ПО.
15. Вредоносное ПО. Виды и классификация вирусов.
16. Жизненный цикл компьютерных вирусов.
17. Классификация вирусов по типу вредоносной нагрузки.
18. Основные угрозы целостности.
19. Законодательный уровень и стандарты ИБ.
20. Группы мер на законодательном уровне.
21. Обзор законодательства РФ в области ИБ.
22. Оценочные стандарты и технические спецификации.
23. ИБ распределенных систем. Рекомендации X.800

24.Распределение функций безопасности по уровням эталонной семиуровневой модели OSI.
25.Обзор сетевые механизмы безопасности.
26.Основные понятия идентификации и аутентификации.
27.Принципы аутентификации.
28.Административный уровень ИБ. Основные понятия.
29.Политика безопасности. Основные понятия.
30.Уровни политики безопасности.
31.Аспекты политики безопасности среднего уровня.
32.Логическое управление доступом.
33.Управление доступом. Матрица доступа.
34.Принцип децентрализации логического управления.
35.Управление доступом. Списки доступа.
36.Произвольное управление доступом.
37.Ролевое управление доступом. Основные понятия.
38.Ролевое управление доступом. Категории функции.
39.Аудит.
40.Активный аудит.
41.Протоколирование.
42.Шифрование. Асинхронное шифрование.
43.Шифрование. Синхронное шифрование.
44.Контроль целостности.
45.Цифровые сертификаты.
46.Экранирование.
47.Классификация межсетевых экранов.

Критерии оценки экзамена

Сумма баллов	**Оценка (ECTS)**	**Оценка (балл за ответ на экзамене)**	**Характеристика знаний студентов**
90-100	A	Отлично	теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному
85 - 89	B	Очень хорошо	теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.
75 - 84	C	Хорошо	теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.

65 - 74	D	Удовлетворительно	теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.
60-64	E	Посредственно	теоретическое содержание курса освоено частично, некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены, либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному
Ниже 60	F	Неудовлетворительно	очень слабые знания, недостаточные для понимания курса, имеется большое количество основных ошибок и недочетов

Учебно-методическое и информационное обеспечение учебной дисциплины

Основная литература:

1. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 400 с. — ISBN 978-5-507-49250-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414947

2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : НГТУ, 2018. — 79 с. https://e.lanbook.com/reader/book/118233/#1

3. Лагоша, О. Н. Сертификация информационных систем : учебное пособие / О. Н. Лагоша. — Санкт-Петербург : Лань, 2020. — 112 с. https://e.lanbook.com/reader/book/139268/#108

4. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. https://e.lanbook.com/reader/book/152227/#1

5. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. https://e.lanbook.com/reader/book/114688/#1

Дополнительная литература:

6. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие для спо / Р. Н. Гилязова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 44 с. https://e.lanbook.com/book/173796

7. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889

Программное обеспечение и Интернет-ресурсы:

1. Электронно-библиотечная система «Лань» - http://e.lanbook.com.
2. Электронно-библиотечная система «Юрайт» - http://www.biblio-onlain.ru.
3. Российская национальная библиотека - http://www.nlr.ru/
4. Поисковая система - http://www.rambler.ru.
5. Поисковая система - http://www.yandex.ru.

6. Гарант - http://base.garant.ru/.
7. Интернет-Университет Информационных Технологий -http://www.intuit.ru

Для проведения практических занятий и выполнения самостоятельной работы используются учебные компьютерные классы с выходом в Интернет и лицензионным программным обеспечением.

Материально-техническое обеспечение учебной дисциплины

Лекционные занятия проводятся в аудиториях: учебная мебель, учебная доска, комплект мультимедийного оборудования

Практические занятия проводятся в компьютерных классах: учебная мебель, учебная доска, комплект мультимедийного оборудования, персональные компьютеры.

Для самостоятельной работы обучающихся имеется: читальный зал с выходом в сеть Интернет: Учебная мебель, комплект мультимедийного оборудования, персональные компьютеры, МФУ.

Учебно-методические рекомендации для студентов

1. Указания для прослушивания лекций

Перед началом занятий внимательно ознакомиться с учебным планом проведения лекций и списком рекомендованной литературы.

Перед посещением очередной лекции освежить в памяти основные концепции пройденного ранее материала. Подготовить при необходимости вопросы преподавателю. Не надо опасаться, что вопросы могут быть простыми.

На лекции основное внимание следует уделять не формулам и математическим выкладкам, а содержанию изучаемых вопросов, определениям и постановкам задач.

В процессе изучения лекционного курса необходимо по возможности часто возвращаться к основным понятиям и методам решения задач (здесь возможен выборочный контроль знаний студентов).

Желательно использовать конспекты лекций, в которых используется принятая преподавателем система обозначений.

Для более подробного изучения курса следует работать с рекомендованными литературными источниками и вновь появляющимися источниками.

2. Указания для участия в практических занятиях

Перед посещением уяснить тему практического занятия и самостоятельно изучить теоретические вопросы.

В конце занятия при необходимости выяснить у преподавателя неясные вопросы.

Основные результаты выполнения работы необходимо оформлять в виде бумажных отчётов.

3. Самостоятельная работа студентов обычно складывается из нескольких составляющих:

- работа с текстами: учебниками, историческими первоисточниками, дополнительной литературой, в том числе материалами интернета, а также проработка конспектов лекций;
- написание докладов, рефератов;
- подготовка к практическим занятиям;

- подготовка к экзамену непосредственно перед ним.

Таким образом, самостоятельная работа студентов является необходимым компонентом получения полноценного высшего образования.

Методические рекомендации для преподавателей

1. Указания для проведения лекций

На первой вводной лекции сделать общий обзор содержания курса и отметить новые методы и подходы к решению задач, рассматриваемых в курсе, довести до студентов требования кафедры, ответить на вопросы.

При подготовке к лекционным занятиям необходимо продумать план его проведения, содержание вступительной, основной и заключительной части лекции, ознакомиться с новинками учебной и методической литературы, публикациями периодической печати по теме лекционного занятия. Уточнить план проведения семинарского занятия по теме лекции. Перед изложением текущего лекционного материала напомнить об основных итогах, достигнутых на предыдущих лекциях. С этой целью задать несколько вопросов аудитории и осуществить выборочный контроль знания студентов.

В ходе лекционного занятия преподаватель должен назвать тему, учебные вопросы, ознакомить студентов с перечнем основной и дополнительной литературы по теме занятия. Раскрывая содержание учебных вопросов, акцентировать внимание студентов на основных категориях, явлениях и процессах, особенностях их протекания. Раскрывать сущность и содержание различных точек зрения и научных подходов к объяснению тех или иных явлений и процессов.

Следует аргументировано обосновать собственную позицию по спорным теоретическим вопросам. Приводить примеры. Задавать по ходу изложения лекционного материала риторические вопросы и самому давать на них ответ. Это способствует активизации мыслительной деятельности студентов, повышению их внимания и интереса к материалу лекции, ее содержанию. Преподаватель должен руководить работой студентов по конспектированию лекционного материала, подчеркивать необходимость отражения в конспектах основных положений изучаемой темы, особо выделяя, категориальный аппарат. В заключительной части лекции необходимо сформулировать общие выводы по теме, раскрывающие содержание всех вопросов, поставленных в лекции. Объявить план очередного практического занятия, дать краткие рекомендации по подготовке студентов к семинару. Определить место и время консультации студентам, пожелавшим выступить на семинаре с докладами и рефератами.

На последней лекции уделить время для обзора наиболее важных положений, рассмотренных в курсе.

2. Указания для проведения практических занятий

Четко обозначить тему практического занятия.

Обсудить основные понятия, связанные с темой практического занятия.

В процессе решения задач вести дискуссию со студентами о правильности применения теоретических знаний.

Отмечать студентов, наиболее активно участвующих в решении задач и дискуссиях.

В конце практического занятия задать аудитории несколько контрольных вопросов.

3.Указания по контролю самостоятельной работы студентов

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

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе.

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

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

Программа составлена в соответствии с требованиями ОС НИЯУ МИФИ по направлению 09.03.02 Информационные системы и технологии

Рабочую программу составил ст. преподаватель кафедры И.В. Михеев

Рецензент: Ю.А. Мефёдова

Программа одобрена на заседании УМКН «Информационные системы и технологии».

Председатель учебно-методической комиссии О.В. Виштак