МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ – МСХА
имени К.А. ТИМИРЯЗЕВА
(ФГБОУ ВО РГАУ - МСХА имени К.А. Тимирязева)

КАЛУЖСКИЙ ФИЛИАЛ

Факультет экономический
Кафедра информационных технологий, учета и экономической безопасности

УТВЕРЖДАЮ:
И.о зам. директора по учебной работе
_____ Т.Н. Пимкина
"23" 05 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.08 Аналитические инструменты обеспечения информационной безопасности

для подготовки специалистов

ФГОС ВО

Специальность 38.05.01 «Экономическая безопасность»
Специализация: «Экономико-правовое обеспечение экономической безопасности»

Курс 3
Семестр 6

Форма обучения: очная, заочная

Год начала подготовки: 2023

Калуга, 2023

Разработчик (и): Гаранина И.Ю.
(ФИО, ученая степень, ученое звание)

«_17» мая___ 2023_г.

Программа составлена в соответствии с требованиями ФГОС ВО, ОПОП по специальности: 38.05.01 Экономическая безопасность и учебным планом

Программа обсуждена на заседании кафедры информационных технологий, учета и экономической безопасности
протокол № 10__ от «_18 _» __мая__2023 г.

Зав. кафедрой _Кокорев Н.А., к.э.н., доцент_____
(ФИО, ученая степень, ученое звание) (подпись)

«_ 18_» __мая____2023_г.

Согласовано:
Председатель учебно-методической комиссии экономического факультета по специальности: 38.05.01 Экономическая безопасность
Негода В.А., к.э.н., доцент_____
(ФИО, ученая степень, ученое звание) (подпись)

«_ 22_» мая 2023_г.

Заведующий выпускающей кафедрой информационных технологий, учета и экономической безопасности

Кокорев Н. А., к.э.н., доцент _____
(ФИО, ученая степень, ученое звание) (подпись)

«_22 _» мая___ 2023 г.

Проверено:

Начальник УМЧ _____ доцент О.А. Окунева

Содержание

АННОТАЦИЯ

рабочей программы учебной дисциплины

Б1.В.08 Аналитические инструменты обеспечения информационной безопасности ОПОП ВО по специальности 38.05.01 – Экономическая безопасность, специализация Экономико-правовое обеспечение экономической безопасности

Цель освоения дисциплины: является формирование у студентов профессионального мышления путем освоения методологических основ и приобретения практических навыков в области аналитических инструментов обеспечения информационной безопасности, необходимых в практической работе. Научится применять в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации такие программные продукты как Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

Место дисциплины в учебном плане. Дисциплина включена в дисциплины вариативной части учебного плана направления подготовки 38.05.01 «Экономическая безопасность» специализация: «Экономико-правовое обеспечение экономической безопасности».

Требования к результатам освоения дисциплины. В результате освоения дисциплины формируются следующие компетенции:

Профессиональные (ПКос):

ПКос-2 – способен анализировать информацию, с использованием информационных систем (программных продуктов) и искусственного интеллекта; выявлять причинно-следственные связи и расставлять приоритеты для дальнейших планов;

- ПКос-2.1– знать методы поиска, сбора, анализа и систематизации информации с использованием информационных систем (программных продуктов) и искусственного интеллекта; оценки и управления рисками внутрикорпоративных злоупотреблений при функционировании вида деятельности, бизнес-модели, процессов и процедур организации;
- ПКос-2.2– уметь анализировать с использованием информационных систем (программных продуктов) и искусственного интеллекта, оценивать и выявлять причинно-следственные связи в порядке функционирования вида деятельности, бизнес-модели, процессов и процедур организации для планирования проверки, разрабатывать регламентирующие документы по управлению рисками;
- ПКос-2.3 – владеть навыками подготовки отчетов по результатам идентификации, анализа, оценки рисков объекта проверки с использованием информационных систем (программных продуктов) и искусственного интеллекта.

Краткое содержание дисциплины: Место и роль аналитических инструментов в системе обеспечении налоговой безопасности организации. Информационное обеспечение аналитических процедур. Правовое обеспечение информационной безопасности. Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации. Уровни информационной безопасности. Аналитические инструменты управления рисками информационной безопасности. Вредоносное программное обеспечение. Организация средств защиты информации

Общая трудоемкость дисциплины: 3 зачетных единиц (108 часов).

Промежуточный контроль: зачет.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины Б1.В.08 «Аналитические инструменты обеспечения информационной безопасности» является формирование у студентов профессионального мышления путем освоения методологических основ и приобретения практических навыков в области аналитических инструментов обеспечения информационной безопасности, необходимых в практической работе. Научится применять в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации такие программные продукты как Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

2. МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Дисциплина «Аналитические инструменты обеспечения информационной безопасности» реализуется в соответствии с требованиями ФГОС ВО, ОПОП ВО и Учебного плана по специальности 38.05.01 Экономическая безопасность.

Предшествующими курсами, на которых непосредственно базируется дисциплина « Аналитические инструменты обеспечения информационной безопасности» являются « Статистика», « Бухгалтерский учет», « Налоги и налогообложение».

Дисциплина «Аналитические инструменты обеспечения информационной безопасности» является основополагающей для изучения следующих дисциплин: «Аналитические инструменты обеспечения инвестиционной безопасности», «Организация деятельности службы безопасности предприятий АПК», «Моделирование угроз и рисков в экономической безопасности».

Особенностью дисциплины «Аналитические инструменты обеспечения информационной безопасности» является комплексный подход при ее изучении и прикладная направленность, позволяющая применять полученные знания по оценке и управлению различными видами рисков в рамках обеспечения экономической безопасности хозяйствующих субъектов.

Рабочая программа дисциплины «Аналитические инструменты обеспечения информационной безопасности» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций, представленных в таблице 1.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
1	ПКос-2	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ПКос-2.1– знать методы поиска, сбора, анализа и систематизации информации с использованием информационных систем (программных продуктов) и искусственного интеллекта; оценки и управления рисками внутрикорпоративных злоупотреблений при функционировании вида деятельности, бизнес-модели, процессов и процедур организации	• и систематизации информации с использованием информационных систем (программных продуктов) и искусственного интеллекта; оценки и управления рисками внутрикорпоративных злоупотреблений при функционировании вида деятельности, бизнес-модели, процессов и процедур организации		
			ПКос-2.2– уметь анализировать с использованием информационных систем (программных продуктов) и искусственного интеллекта, оценивать и выявлять причинно-следственные связи в порядке функционирования вида деятельности, бизнес-модели, процессов и процедур организации для планирования проверки, разрабатывать регламентирующие документы по управлению рисками		• анализировать с использованием информационных систем (программных продуктов) и искусственного интеллекта, оценивать и выявлять причинно-следственные связи в порядке функционирования вида деятельности, бизнес-модели, процессов и процедур организации для планирования проверки, разрабатывать регламенти-	

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
					рующие документы по управлению рисками	
			ПКос-2.3 – владеть навыками подготовки отчетов по результатам идентификации, анализа, оценки рисков объекта проверки с использованием информационных систем (программных продуктов) и искусственного интеллекта			• навыками подготовки отчетов по результатам идентификации, анализа, оценки рисков объекта проверки с использованием информационных систем (программных продуктов) и искусственного интеллекта

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 часов), их распределение по видам работ семестрам представлено в таблицах 2а и 2б.

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2а

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час. всего	**В т.ч. по семестрам**
		№ 6
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**54**	**54**
Аудиторная работа	**54**	**54**
в том числе:		
лекции (Л)	18	18
практические занятия (ПЗ)	36	36
2. Самостоятельная работа (СРС)	**54**	**54**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала, подготовка к практическим занятиям)	45	45
подготовка к промежуточной аттестации	9	9
Вид промежуточного контроля:	зачёт	зачёт

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 2б

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час.	**В т.ч. по семестрам**
		№6
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**12**	**12**
Аудиторная работа	**12**	**12**
в том числе:		
лекции (Л)	6	6
практические занятия (ПЗ)	6	6
2. Самостоятельная работа (СРС)	**92**	**92**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям, коллоквиумам и т.д.)	92	92
Контроль (подготовка к зачету)	**4**	**4**
Вид промежуточного контроля	зачёт	

4.2 Содержание дисциплины

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3а

Тематический план учебной дисциплины

Наименование разделов и тем дисциплин (укрупнённо)	Всего	Контактная работа		Внеаудиторная работа СР
		Л	ПЗ	
Тема 1. Место и роль аналитических инструментов в системе обеспечении информационной безопасности организации	12	2	4	6
Тема 2. Правовое обеспечение информационной безопасности	12	2	4	6
Тема 3. Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты.	12	2	4	6
Тема 4. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	12	2	4	6
Тема 5. Уровни информационной безопасности	12	2	4	6
Тема 6. Аналитические инструменты управления рисками информационной безопасности	20	4	6	10
Тема 7. Вредоносное программное обеспечение	16	2	6	8
Тема 8. Организация средств защиты информации	12	2	4	6
Итого по дисциплине	**108**	**18**	**36**	**54**

Тема 1. Место и роль аналитических инструментов в системе обеспечении налоговой безопасности организации

Понятие и содержание информационной деятельности. Понятие и виды экономических инструментов, рычагов управления информационным пространством организации. Понятие и виды аналитических инструментов. Цели и задачи аналитических инструментов в обеспечении информационной безопасности хозяйствующего субъекта. Инструменты идентификации угроз и рисков информационной безопасности организаций АПК. Субъекты и объекты системного анализа. Цели, задачи и интересы различных субъектов. Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

Тема 2. Правовое обеспечение информационной безопасности

Информационная база для проведения аналитических процедур. Сущность и виды информации. Понятие информационная безопасность. Основные составляющие. Актуальность и проблемы информационной безопасности хозяйствующих субъектов. Содержание и роль источников информации. Первичная аналитическая обработка информации. Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

Тема 3. Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты

Объектно-ориентированный подход к информационной безопасности. Физическая

защита объектов. Концепция построения систем защиты. Сложные системы. Технические средства охраны. Основные принципы построения защиты. Классы каналов несанкционированного доступа. Основные задачи систем защиты. Стойкость алгоритма шифрования Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

Тема 4. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации

Основные определения и критерии классификации угроз. Меры противодействия угрозам. Принципы построения систем защиты. Классификация угроз. Целостность программного обеспечения. Оценочные стандарты и технические спецификации. Критерии оценки степени доверия. Политика безопасности. Уровень гарантированности. Механизм подотчетности (протоколирования). Доверенная вычислительная база. Механизмы безопасности. Виды гарантированности. Классы безопасности. Администрирование средств безопасности. Администрирование сервисов безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

Тема 5. Уровни информационной безопасности

Уровни информационной безопасности: законодательный, административный, процедурный, программно-технический. Конституция РФ. Доктрина информационной безопасности РФ. Основные принципы доктрины. Уголовный кодекс РФ. Закон "Об информации, информатизации и защите информации" Основные положения. Закон «О лицензировании отдельных видов деятельности». Закон "Об электронной цифровой подписи". Закон «О персональных данных». ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Единый реестр запрещенных сайтов. Административный уровень информационной безопасности. Политика безопасности. Анализ рисков. Программа безопасности. Процедурный уровень информационной безопасности. Программно-технический уровень информационной безопасности. Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

Тема 6. Аналитические инструменты управления рисками информационной безопасности.

Классификация аналитических инструментов управления рисками информационной безопасности. Система управления рисками. Риск-менеджер. Этапы управления рисками. Идентификация рисков. Категоризация рисков. Этап мониторинга анализа эффективности управления рисками. Обновление базы известных рисков. Паспортизация рисков. SWOT-анализ. Классификация рисков. Классификация проектов по рискам. Критерии риск-менеджера. Анализ эффективности управления рисками. Критерии эффективности управления рисками Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

Тема 7. Вредоносное программное обеспечение

Типы вредоносного программного обеспечения. История компьютерных вирусов. Признаки присутствия на компьютере вредоносного программного обеспечения. Грани вредоносного программного обеспечения. Классификация по вредоносной функции. Загрузочные вирусы. MBR вирусы. Файловые вирусы. Сетевые черви. Троянские программы. Макровирусы. Резидентные вирусы. Резидентные вирусы. Самошифрование и полиморфизм. Особенности современного вредоносного программного обеспечения. Хакерские утилиты и другое вредоносное программное обеспечение. Виды проявления вредоносного программного обеспечения. Сетевая активность. Защита от вредоносных программ. Методы защиты от вредоносных программ. Самозащита вредоносного программ-

ного обеспечения. Полиморфизм и обфускация. Борьба с антивирусами. Направления самозащиты. Типы антивирусов. Правила обработки информации. Применение в коммуникационном процессе для ускорения передачи, обработкии интерпретации финансовой информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

Тема 8. Организация средств защиты информации

Атаки. Виды атак. Локальные атаки. Средства аутентификации. Получение доступа на этапе загрузки ОС. Методы защиты. Социальная инженерия. Классификация удаленных атак. Межсетевой экран. Брандмауэры. Характеристики фаерволов. Управляемые коммутаторы канального уровня. Шлюзы сеансового уровня. Шлюзы прикладного уровня. Классификация по отслеживанию соединений. Режим секретности. Основные понятия. Государственная тайна. Признаки государственной тайны. Секретность. Элементы режима секретности. Грифы секретности и формы допуска. Защита государственной тайны. Порядок работы с секретными документами. Криптология. Крипто анализ. История криптографии. Полиалфавитные шифры. Шифр Виженера. Шифр Гронсфельда. Энигма. Современная криптография. Классификация криптоалгоритмов. Перестановочные алгоритмы. Потоковые шифры. Симметричные алгоритмы. Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP.

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 3б

Тематический план учебной дисциплины

Наименование разделов и тем дисциплин (укрупнённо)	**Всего**	**Контактная работа**		**Внеаудиторная работа СР**
		Л	**ПЗ**	
Тема 1. Место и роль аналитическихинструментов в системе обеспечении информационной безопасности организации	14	2	-	12
Тема 2. Правовое обеспечение информационной безопасности	14	2	-	12
Тема 3. Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты.	12	-	-	12
Тема 4. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	14	2	-	12
Тема 5. Уровни информационной безопасности	12	-	-	12
Тема 6. Аналитические инструменты управления рисками информационной безопасности	14	-	2	12
Тема 7. Вредоносное программное обеспечение	14	-	2	12
Тема 8. Организация средств защиты информации	14	-	2	12
Итого по дисциплине	**108**	**6**	**6**	**96***

4.3 Лекции / практические занятия

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

* В том числе подготовка к экзамену (контроль)

Таблица 4а

Содержание лекций / практических занятий и контрольные мероприятия

№ п/п	№ темы	№ и название лекций/ практических/ занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов
1.	Тема 1. Место и роль аналитическихинструментов в системе обеспечении информационной безопасности организации	Лекция №1 Место и роль аналитических инструментов в системе обеспечении информационной безопасности организации	Пкос-2.1; Пкос-2.2; Пкос-2.3	устный опрос, защита практической работы	2
		Практическая работа №1 Место и роль аналитических инструментов в системе обеспечении информационной безопасности организации	Пкос-2.1; Пкос-2.2; Пкос-2.3		4
2.	Тема 2. Правовое обеспечение информационной безопасности	Лекция №2 Правовое обеспечение информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	2
		Практическая работа №2 Правовое обеспечение информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3		4
3.	Тема 3. Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты.	Лекция №3 Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты.	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	2
		Практическая работа №3 Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты.	Пкос-2.1; Пкос-2.2; Пкос-2.3		4
4.	Тема 4. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	Лекция №4 Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	2
		Практическая работа №4 Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	Пкос-2.1; Пкос-2.2; Пкос-2.3		4

№ п/п	№ темы	№ и название лекций/ практических/ занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов
5.	Тема 5. Уровни информационной безопасности	Лекция №5 Уровни информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3		2
		Практическая работа №5 Уровни информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	4
6.	Тема 6. Аналитические инструменты управления рисками информационной безопасности	Лекция №6 Аналитические инструменты управления рисками информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	4
		Практическая работа №6 Аналитические инструменты управления рисками информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3		6
7.	Тема 7. Вредоносное программное обеспечение	Лекция №7 Вредоносное программное обеспечение	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	2
		Практическая работа №7 Вредоносное программное обеспечение	Пкос-2.1; Пкос-2.2; Пкос-2.3		6
8.	Тема 8. Организация средств защиты информации	Лекция №8 Организация средств защиты информации	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы, тестирование	2
		Практическая работа №8 Организация средств защиты информации	Пкос-2.1; Пкос-2.2; Пкос-2.3		4

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 4б

Содержание лекций / практических занятий и контрольные мероприятия

№ п/п	№ темы	№ и название лекций/ практических/ занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов
1.	Тема 1. Место и роль аналитическихинструментов в системе обеспечении информационной безопасности организации	Лекция №1 Место и роль аналитических инструментов в системе обеспечении информационной безопасности организации	Пкос-2.1; Пкос-2.2; Пкос-2.3	устный опрос	2

№ п/п	№ темы	№ и название лекций/ практических/ занятий	Формируемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов
2.	Тема 2. Правовое обеспечение информационной безопасности	Лекция №2 Правовое обеспечение информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3	устный опрос	2
3.	Тема 4. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	Лекция №4 Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	Пкос-2.1; Пкос-2.2; Пкос-2.3	устный опрос	2
4.	Тема 6. Аналитические инструменты управления рисками информационной безопасности	Практическая работа №6 Аналитические инструменты управления рисками информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	2
5.	Тема 7. Вредоносное программное обеспечение	Практическая работа №7 Вредоносное программное обеспечение	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	2
6.	Тема 8. Организация средств защиты информации	Практическая работа №8 Организация средств защиты информации	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы, тестирование	2

ОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 5а

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	№ раздела и темы	Перечень рассматриваемых вопросов длясамостоятельного изучения
1.	Тема 1. Место и роль аналитическихинструментов в системе обеспечении информационной безопасно-	Схема информационной безопасности организации. Особенности информационного анализа с точки зрения разных субъектов анализа (Пкос-2.1; Пкос-2.2; Пкос-2.3.)

№ п/п	№ раздела и темы	Перечень рассматриваемых вопросов длясамостоятельного изучения
	сти организации	
2.	Тема 2. Правовое обеспечение информационной безопасности	Основные подходы к созданию системы защиты информации, технические средства защиты информации, методы защиты информации (Пкос-2.1; Пкос-2.2; Пкос-2.3.)
3.	Тема 3. Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты.	Основные принципы правового регулирования отношений, возникающих в сфере информации. Федеральный закон «Об информации, технологиях и защите информации». Федеральный закон «О коммерческой тайне». Перечень информации (сведений), составляющей коммерческую тайну. Степени секретности, установленные в РФ (Пкос-2.1; Пкос-2.2; Пкос-2.3.)
4.	Тема 4. Основные определения и критерииклассификации угроз. Оценочные стандарты и технические спецификации	Основные направления аналитической работы по предупреждению утечки конфиденциальной информации. Основные функции аналитического подразделения. Классификация методов анализа информации. (Пкос- 2.1; Пкос-2.2; Пкос-2.3.)
5.	Тема 5. Уровни информационной безопасности	Функции контрольно-пропускного режима. Основные цели контрольно-пропускного режима. Исходные данные необходимые для разработки мероприятий и нормативных документов контрольно-пропускного режима. (Пкос-2.1; Пкос-2.2; Пкос-2.3.)
6.	Тема 6. Аналитические инструменты управления рисками информационной безопасности	Работа с персоналом предприятия, имеющим доступ к конфиденциальной информации. Основные причины разглашения конфиденциальной информации допущенным к ней персоналом предприятия. Обязанности работодателя по отношению к сотруднику предприятия в связи с охраной конфиденциальности информации (Пкос-2.1; Пкос-2.2; Пкос-2.3.)
7.	Тема 7. Вредоносное программное обеспечение	Допуск к конфиденциальной информации. Меры по охране конфиденциальности информации (Пкос-2.1; Пкос-2.2; Пкос-2.3)
8.	Тема 8. Организация средств защиты информации	Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций. Контроль функционирования системы организационной защиты информации (Пкос-2.1; Пкос-2.2; Пкос-2.3.)

ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ

Таблица 5б

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	№ раздела и темы	Перечень рассматриваемых вопросов длясамостоятельного изучения
1.	Тема 1. Место и роль аналитическихинструментов в системе обеспечении информационной безопасно-	Схема информационной безопасности организации. Особенности информационного анализа с точки зрения разных субъектов анализа (Пкос-2.1; Пкос-2.2; Пкос-2.3.)

№ п/п	№ раздела и темы	Перечень рассматриваемых вопросов длясамостоятельного изучения
	сти организации	
2.	Тема 2. Правовое обеспечение информационной безопасности	Основные подходы к созданию системы защиты информации, технические средства защиты информации, методы защиты информации (Пкос-2.1; Пкос-2.2; Пкос-2.3.)
3.	Тема 3. Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты.	Основные принципы правового регулирования отношений, возникающих в сфере информации. Федеральный закон «Об информации, технологиях и защите информации». Федеральный закон «О коммерческой тайне». Перечень информации (сведений), составляющей коммерческую тайну. Степени секретности, установленные в РФ (Пкос-2.1; Пкос-2.2; Пкос-2.3.)
4.	Тема 4. Основные определения и критерииклассификации угроз. Оценочные стандарты и технические спецификации	Основные направления аналитической работы по предупреждению утечки конфиденциальной информации. Основные функции аналитического подразделения. Классификация методов анализа информации. (Пкос- 2.1; Пкос-2.2; Пкос-2.3.)
5.	Тема 5. Уровни информационной безопасности	Функции контрольно-пропускного режима. Основные цели контрольно-пропускного режима. Исходные данные необходимые для разработки мероприятий и нормативных документов контрольно-пропускного режима. (Пкос-2.1; Пкос-2.2; Пкос-2.3.)
6.	Тема 6. Аналитические инструменты управления рисками информационной безопасности	Работа с персоналом предприятия, имеющим доступ к конфиденциальной информации. Основные причины разглашения конфиденциальной информации допущенным к ней персоналом предприятия. Обязанности работодателя по отношению к сотруднику предприятия в связи с охраной конфиденциальности информации (Пкос-2.1; Пкос-2.2; Пкос-2.3.)
7.	Тема 7. Вредоносное программное обеспечение	Допуск к конфиденциальной информации. Меры по охране конфиденциальности информации (Пкос-2.1; Пкос-2.2; Пкос-2.3)
8.	Тема 8. Организация средств защиты информации	Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций. Контроль функционирования системы организационной защиты информации (Пкос-2.1; Пкос-2.2; Пкос-2.3.)

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Тема и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
1	Тема 1. Место и роль аналитических инструментов в системе обеспечении информационной безопасности организации	ПЗ	Технология активного обучения (ситуационные задания)

2	Тема 2. Правовое обеспечение информационной безопасности	ПЗ	Технология активного обучения (ситуационные задания)
3	Тема 3. Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты.	ПЗ	Технология активного обучения (ситуационные задания)
4	Тема 4. Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	ПЗ	Технология активного обучения (ситуационные задания)
5	Тема 5. Уровни информационной безопасности	ПЗ	Технология активного обучения (ситуационные задания)
6	Тема 6. Аналитические инструменты управления рисками информационной безопасности	ПЗ	Технология активного обучения (ситуационные задания)
7	Тема 7. Вредоносное программное обеспечение	ПЗ	Технология активного обучения (ситуационные задания)
8	Тема 8. Организация средств защиты информации	ПЗ	Технология активного обучения (ситуационные задания)

6. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

6.1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

Типовые тесты по дисциплине «Аналитические инструменты обеспечения информационной безопасности»

1. Незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, наносящий ее владельцу ущерб, — это...

1) политическая разведка;
2) промышленный шпионаж;
3) добросовестная конкуренция;
4) конфиденциальная информация;
5) правильного ответа нет.

2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?

1) любая информация;
2) только открытая информация;
3) запатентованная информация;
4) закрываемая собственником информация;
5) коммерческая тайна.

3. Кто может быть владельцем защищаемой информации?

1) только государство и его структуры;
2) предприятия акционерные общества, фирмы;
3) общественные организации;
4) только вышеперечисленные;
5) кто угодно.

4. Какие сведения на территории РФ могут составлять коммерческую тайну?

1) учредительные документы и устав предприятия;
2) сведенья о численности работающих, их заработной плате и условиях труда;
3) документы о платежеспособности, об уплате налогов, о финансово- хозяйственной деятельности;
4) другие;
5) любые.

5. Какие секретные сведения входят в понятие «коммерческая тайна»?

1) связанные с производством;
2) связанные с планированием производства и сбытом продукции;
3) технические и технологические решения предприятия;
4) только 1 и 2 вариант ответа;
5) три первых варианта ответа.

6. Что называют источником конфиденциальной информации?

1) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников;
2) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;
3) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;
4) это защищаемые предприятием сведения в области производства и коммерческой деятельности;
5) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.

7. Как называют процессы обмена информацией с помощью официальных, деловых документов?

1) непосредственные;
2) межличностные;
3) формальные;
4) неформальные;
5) конфиденциальные.

Типовые практические задания по практике дисциплины «Аналитические инструменты обеспечения налоговой безопасности»

1. Законодательство РФ в области информационной безопасности
2. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации
3. Система сертификации средств криптографической защиты информации
4. Изучение положения о сертификации средств вычислительной техники и связи
5. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации
6. Изучение особенностей аттестации помещений по требованиям безопасности информации

7. Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации
8. Изучение типового положения об испытательной лаборатории
9. Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации
10. Изучение положений о государственном лицензировании деятельности в области защиты информации

Перечень вопросов, выносимых на промежуточную аттестацию (зачет).

1. Понятие и виды аналитических инструментов в обеспечении информационной безопасности хозяйствующего субъекта
2. Информационная база для проведения аналитических процедур
3. Организационное обеспечение информационной безопасности как составная часть системы комплексного противодействия информационным угрозам
4. Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране
5. Основные принципы построения организационного обеспечения защиты информации и предъявляемые к ней требования
6. Основные цели и задачи организационного обеспечения информационной безопасности на предприятии
7. Объекты и субъекты организационного обеспечения защиты информации коммуникативного процесса
8. Угрозы информационной безопасности. Виды угроз. Организационныемеры противодействия различным видам угроз
9. Случайные и преднамеренные угрозы. Меры организационного противодействия случайным и преднамеренным угрозам
10. Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ
11. Классификация каналов утечки информации относительно возможных действий нарушителя информационной безопасности
12. Содержание аналитических документов, необходимых для разработки «Политики информационной безопасности предприятия»
13. Структура и содержание документа «Политика информационной безопасности предприятия»
14. Служба информационной безопасности предприятия. Состав, цели и задачи службы информационной безопасности предприятия
15. Концепция информационной безопасности предприятия. Цели и задачи предприятия в обеспечении информационной безопасности при взаимодействии с внешними и внутренними субъектами информационного обмена
16. Роль стандартов и требований по информационной безопасности предприятия в формировании «Политики информационной безопасности предприятия»
17. Процедуры и методы информационной безопасности предприятия как составляющие «Политики информационной безопасности предприятия». Профили защиты
18. Права и обязанности руководящего состава и сотрудников службы информационной безопасности. Роль служебных комиссий и «кризисных групп» в обеспечении информационной безопасности
19. Порядок установления режима конфиденциальности информации. Пере-

чень сведений, относимых к конфиденциальной информации и не подлежащих засекречиванию

20. Организация конфиденциального делопроизводства

21. Общие обязанности сотрудников по неразглашению конфиденциальной информации

22. Организация доступа и допуска сотрудников к конфиденциальной информации

23. Организация доступа к информационным системам, обрабатывающим конфиденциальную информацию. Матричный и мандатный подходы к проблемам разграничения доступа

24. Порядок обеспечения сохранности конфиденциальной информации при постоянном или временном прекращении пользователем доступа к конфиденциальному информационному ресурсу

25. Требования, предъявляемые к претендентам на работу с конфиденциальной информацией и к претендентам на должность службу информационной безопасности

26. Кадровая политика предприятия. Возможные источники пополнения предприятия кадрами для работы с конфиденциальной информацией

27. Порядок организации и проведения конкурсов на замещения вакантных должностей, связанных с безопасностью информации

28. Методы проверки кандидатов на работу. Отражение вопросов информационной безопасности в трудовых и коллективных договорах

29. Текущая работа с персоналом, допущенным к конфиденциальной информации. Дисциплинарная ответственность. Меры поощрения и наказания

30. Методы борьбы с нарушениями информационной безопасности. Порядок завершения текущей работы с сотрудниками, владеющими конфиденциальной информацией при их увольнении

31. Организация служебного расследования по фактам утечки конфиденциальной информации. Порядок проведения служебного расследования по фактамутраты секретных документов и разглашения конфиденциальной информации

32. Сложные инциденты. Порядок организации служебного расследования в случаях возникновения сложных инцидентов

33. Организация охраны объектов информатизации. Составные элементы системы охраны. Требования к охранникам и их обязанностям

34. Организация режима охраны объекта. Принципы охраны. Факторы, влияющие на выбор приёмов и средств охраны

35. Организация внутриобъектового и пропускного режимов на объектах информатизации. Цели организации внутриобъктового режима

36. Зона режимности предприятия. Требования к введению внутриобъктового режима

37. Организация пропускного режима. Типы пропусков. Учёт пропускных документов

38. Атрибутивный и биометрический способы идентификации сотрудников. Их преимущества и недостатки

39. Порядок соблюдения объектового режима при работе с представителями сторонних организаций

40. Возможные каналы утечки информации из помещений, в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия. Требования СТР-К по защите помещений. Организация борьбы с утечкой информации из по-

мещений

41. Аттестация помещений, в которых обрабатывается конфиденциальная информация. Этапы проведения аттестации. Технический паспорт на помещение и аттестат соответствия

42. Порядок организации работ по созданию и эксплуатации объектов информатизации и средств защиты информации (СЗИ), определяемый СТР К. Стадии создания объекты информации

43. Порядок организации эксплуатации автоматизированных систем и их средств защиты информации. Особенности защиты информации при использовании съемных накопителей информации большой емкости для АРМ на базе автономных ЭВМ

44. Порядок защиты информации в СУБД. Защита информации в локальных вычислительных сетях и при выходе в сети общего пользования

45. Организация защиты информации при взаимодействии со сторонниками организациями. Порядок отбора и подготовки информации к оглашению. Отражение вопросов защиты информации при подготовке договоров

46. Обеспечение защиты информации при ведении переговоров и при приеме в организации сторонних организаций и посетителей. Особенности обеспечения безопасности информации при приеме иностранных делегаций

47. Роль информационно-аналитической работы как составной части организационных методов защиты информации. Основные показатели качества информации. Методы прогнозирования и верификации

48. Контроль функционирования системы организационной защиты информации. Формы контроля

49. Аудит информационной безопасности. Формы аудита. Особенности аудита автоматизированных информационных систем

50. Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций. Требования пожарной безопасности к объектам информатизации

51. Меры по охране конфиденциальности информации

52. Информационное обеспечение аналитических инструментов обеспечения информационной безопасности (Проведение совещаний при помощи Zoom, обмен информацией посредством системы Google –документов, Outlook, Power Point)

53. Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, 1С: ERP

54. Инструменты моделирования и оптимизации решений Project Expert, Power Point для формирования объективного акта ревизии

6.2. Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Таблица 7

Критерии оценивания результатов обучения

Оценка	Критерии оценивания
зачтено	теоретическое содержание курса освоено полностью, компетенции сформированы, все предусмотренные программой обучения учебные задания выполнены с незначительными замечаниями. Умения и навыки применяются студентом для решения практических задач с незначительными ошибками, исправляемыми студентом самостоятельно.

незачтено	теоретическое содержание курса не освоено, компетенции не сформированы, из предусмотренных программой обучения учебных заданий либо выполнено менее 60%, либо содержит грубые ошибки, приводящие к неверному решению; Умения и навыки студент не способен применить для решения практических задач.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт,2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

2. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

7.2 Дополнительная литература

1. Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534- 12769-0. — Текст: электронный // Образовательная платформа Юрайт [сайт].
— URL: https://urait.ru/bcode/496492

2. Организационное и правовое обеспечение информационной безопасно- сти : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844

3. Северцев, Н. А. Системный анализ теории безопасности: учебное пособие для вузов / Н. А. Северцев, А. В. Бецков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 456 с. — (Высшее образование). — ISBN 978-5-534-07985-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493334

7.3 Нормативные правовые акты

1. Конституция Российской Федерации;
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 №174-ФЗ;
3. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 №95-ФЗ;
4. Кодекс Российской Федерации об административных правонарушениях, от 30 декабря 2001 г. №195-ФЗ;
5. Налоговый кодекс Российской Федерации. Часть первая от 31.107.1998 г. №146-ФЗ и часть 2 от 05.08.2000 №117-ФЗ;
6. Гражданский кодекс РФ. часть первая от 30 ноября 1994 г. №51-ФЗ, часть вторая от 26 января 1996 г. №14-ФЗ, часть третья от 26 ноября 2001 г. №146-ФЗ и часть четвертая от 18 декабря 2006 г. №230-ФЗ;

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Правительство Российской Федерации. – Открытый доступ. – Режим доступа к материалам: http://government.ru.
2. Министерство финансов Российской Федерации. – Режим доступа к материа- лам: https://m.minfin.gov.ru
3. Министерство сельского хозяйства Российской Федерации – Режим доступа к материалам: http://mcx.ru
4. Министерство экономического развития Российской Федерации – Режим до- ступа к материалам: http://economy.gov.ru.
5. Центральная научная библиотека имени Н.И. Железнова. – Режим доступа к материалам: http:// www.library.timacad.ru.

9. ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. СПС Консультант Плюс (http://www.consultant.ru/);

Таблица 8

Перечень программного обеспечения

№ п/п	Наименование раздела учебной дисциплины	Наименование программы	Тип программы	Автор	Год разработки
1.	Все темы дисциплины	Microsoft Office	Офисное приложение	Microsoft	2019
2.	Все темы дисциплины	Project Expert	Программа автоматизации бизнес-планирования	Expert Systems	2009
3.	Все темы дисциплины	1С:ERP	Обучающая	ООО «1С - Учебный центр № 3»	2018

10. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Таблица 9

Сведения об обеспеченности специализированными аудиториями, кабинетами, лабораториями

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	Оснащенность специальных помещений и помещений для самостоятельной работы
Аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивиду-	столы (15 шт.); стулья (30 шт.), доска; мультимедийное оборудование переносное (проектор Acer X1226H, Ноутбук Levono Essential G780) с доступом в Интернет

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	Оснащенность специальных помещений и помещений для самостоятельной работы
альных консультаций, текущего контроля и промежуточной аттестации (2-401)	
Помещение для самостоятельной работы обучающихся (2-406)	компьютерные столы (15 шт.); стулья (15 шт.); рабочее место преподавателя; рабочая станция (моноблок) Lenovo V310z (15 шт.) подключенные к сети Интернет и обеспеченные доступом к ЭБС.

11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ СТУДЕНТАМ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При изучении курса целесообразно придерживаться следующей последовательности:

1. До посещения первой лекции:
   а) внимательно прочитать основные положения программы курса;
   б) подобрать необходимую литературу и ознакомиться с её содержанием.
2. После посещения лекции:
   а) углублено изучить основные положения темы программы по материалам лекции и рекомендуемым литературным источникам;
   б) дополнить конспект лекции краткими ответами на каждый контрольный вопрос к теме;
   в) составить список вопросов для выяснения во время аудиторных занятий;
   г) подготовиться к практическим занятиям (семинарам).

Задания для самостоятельной работы студентов являются составной частью учебного процесса. Выполнение заданий способствует:

- закреплению и расширению полученных студентами знаний по изучаемым вопросам в рамках учебной дисциплины.
- развитию навыков работы с нормативно-правовыми актами.
- развитию навыков обобщения и систематизации информации.

Важность самостоятельной работы студентов обусловлена повышением требований к уровню подготовки специалистов в современных условиях, необходимостью приобретения навыков самостоятельно находить информацию по вопросам информатики в различных источниках, её систематизировать, и давать им оценку.

Самостоятельная работа приобщает студентов к научному творчеству, поиску и решению актуальных современных проблем в сфере информатики.

Задания для самостоятельной работы выполняются студентами во внеаудиторное время.

Виды и формы отработки пропущенных занятий

Студент, пропустивший занятия обязан его отработать. Отработка занятий осуществляется в соответствии с графиком консультаций.

Пропуск лекционного занятия студент отрабатывает самостоятельно и представляет ведущему преподавателю конспект лекций по пропущенным занятиям.

Пропуск практического занятия студент отрабатывает под руководством ведущего преподавателя дисциплины.

12. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПРЕПОДАВАТЕЛЯМ ПО ОРГАНИЗАЦИИ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Для лучшего усвоения материала студентами преподавателю рекомендуется в первую очередь ознакомить их с программой курса и кратким изложением материала курса, представленного в образовательной программе дисциплины. Далее, необходимо ознакомить студентов с основными терминами и понятиями, применяемые в дисциплине. Далее согласно учебному плану на лекционных занятиях преподаватель должен довести до студентов теоретический материал согласно тематике и содержанию лекционных занятий, представленных в рабочей программе.

В лекциях следует приводить разнообразные примеры практических задач, решение которых подкрепляется изучаемым разделом курса.

На занятиях необходимо не только сообщать учащимся те или иные знания по курсу, но и развивать у студентов логическое мышление, расширять их кругозор.

Преподавателю следует ознакомить студентов с графиком проведения консультаций.

Для обеспечения оценки уровня подготовленности студентов следует использовать разнообразные формы контроля усвоения учебного материала. Устные опросы / собеседование позволяют выявить уровень усвоения теоретического материала, владения терминологией курса.

Ведение подробных конспектов лекций способствует успешному овладению материалом. Проверка конспектов применяется для формирования у студентов ответственного отношения к учебному процессу, а также с целью обеспечения дальнейшей самостоятельной работы студентов.

Самостоятельная работа студентов является важнейшей составной частью учебной работы и предназначена для достижения следующих целей:

- закрепление и углубление полученных знаний, умений и навыков;
- подготовка к предстоящим занятиям и зачету;
- формирование культуры умственного труда и самостоятельности в поиске и приобретении новых знаний.

Преподавателям следует объяснить студентам необходимость самостоятельной работы для успешного освоения курса. Средствами обеспечения самостоятельной работы студентов являются учебники, сборники задач и учебные пособия, приведенные в списке основной и дополнительной литературы. Кроме того, студент может использовать Интернет-ресурсы в том числе ЭБС филиала.

Использование новых информационных технологий в цикле лекций и практических занятий по дисциплине позволяют максимально эффективно задействовать и использовать информационный, интеллектуальный и временной потенциал, как студентов, так и преподавателей для реализации поставленных учебных задач. Основной целью практических занятий является: интегрировать знания, полученные по другим дисциплинам данного направления и активизировать их использование, как в случае решения поставленных задач, так и в дальнейшей практической деятельности.

Программу разработал:

Мишин П.Н., к.э.н