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)

Институт экономики и управления АПК
Кафедра экономической безопасности, анализа и аудита

УТВЕРЖДАЮ:
Директор института
экономики и управления АПК
_____ Л.И. Хоружий
“ ” _____ 202_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.10.06 Аналитические инструменты обеспечения информационной безопасности

для подготовки экономистов

ФГОС ВО

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

Курс 3

Семестр 6

Форма обучения очная

Год начала подготовки 2022

Москва, 2022

Разработчики: Катков Ю.Н. к.э.н., доцент, Каткова Е.А., к.э.н., доцент

«01» июня 2022 г.

Рецензент: Хоружий Л.И., д.э.н., профессор

«01» июня 2022 г..

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.05.01 Экономическая безопасность, профессиональных стандартов и учебного плана 2022 года начала подготовки

Программа обсуждена на заседании кафедры экономической безопасности, анализа и аудита
протокол № 11 от «09» июня 2022 г.

И.о. заведующий кафедрой Гупалова Т.Н., к.э.н., доцент

(подпись)

«09» июня 2022 г.

Согласовано:
Председатель учебно-методической
комиссии института экономики и управления АПК
Корольков А.Ф., к.э.н., доцент

(подпись)

протокол № 10 от «30» июня 2022 г.

Заведующий отделом комплектования ЦНБ

СОДЕРЖАНИЕ

АННОТАЦИЯ
рабочей программы учебной дисциплины
Б1.В.10.06 Аналитические инструменты обеспечения информационной безопасности ОПОП ВО по специальности 38.05.01 Экономическая безопасность, специализация Экономико-правовое обеспечение экономической безопасности (квалификация выпускника – экономист)

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, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

Место дисциплины в учебном плане: дисциплина: «Аналитические инструменты обеспечения информационной безопасности» включена в часть формируемую участниками образовательных отношений учебного плана по специальности 38.05.01 «Экономическая безопасность».

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции Пкос-2.1; Пкос-2.2; Пкос-2.3

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 составляет 3 зачетные единицы (108 часов).

Промежуточный контроль по дисциплине: зачет

1. Цель освоения дисциплины

Целью учебной дисциплины «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, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

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 «Системный анализ рисков» являются «Экономическая безопасность», «Профессиональная этика», «Кадровая безопасность организаций АПК».

Дисциплина «Аналитические инструменты обеспечения информационной безопасности» является основополагающей для изучения следующих дисциплин: «Аудит», «Стратегический анализ в обеспечении экономической безопасности организаций АПК», «Контроль и ревизия», а также практики по получению профессиональных умений и опыта профессиональной деятельности, производственной практики по получению профессиональных умений и опыта профессиональной деятельности и первичных умений и навыков научно-исследовательской деятельности, преддипломной практики.

Особенностью дисциплины «Аналитические инструменты обеспечения налоговой 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	Индекс компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				Знать	Уметь	Владеть
1.	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	- угрозы и риски информационной безопасности хозяйствующего субъекта; - возможности интернет ресурсов и программных продуктов при решении профессиональных задач (Консультант, Гарант, официальные сайты министерств и ведомств, Nalog.ru, CRM, ERP системы, Бизнес-навигатор МСП).		
			Пкос-2.2 Уметь анализировать с использованием информационных систем (программных продуктов) и искусственного интеллекта, оценивать и выявлять причинно-следственные связи в порядке функционирования		- идентифицировать угрозы и риски информационной безопасности хозяйствующего субъекта; - разрабатывать локальные нормативные акты, регламентирующие деятельность по обеспечению информацион-	

№ п/п	Индекс компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				Знать	Уметь	Владеть
			цедур организации для планирования проверки, разрабатывать регламентирующие документы по управлению рисками		ной безопасности хозяйствующего субъекта; - распределять профессиональные задач в системе Битрикс24;	
			Пкос-2.3 Владеть навыками подготовки отчетов по результатам идентификации, анализа, оценки рисков объекта проверки с использованием информационных систем (программных продуктов) и искусственного интеллекта			- способами идентификации угроз и рисков информационной безопасности хозяйствующего субъекта; - положениями нормативно-правовых актов, регламентирующих деятельность по обеспечению информационной безопасности хозяйствующего субъекта; - навыками поиска информации посредством электронных ресурсов (Яндекс, Mail, Бизнес-навигатор МСП), официальных сайтов различных ведомств.

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов), их распределение по видам работ представлено в таблице 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	всего/*	**в т.ч. в семестре №6**
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**50,35/4**	**50,35/4**
Аудиторная работа	**50,35/4**	**50,35/4**
в том числе:		
лекции (Л)	16	16
практические занятия (ПЗ)	34/4	34/4
контактная работа на промежуточном контроле (КРА)	0,35	0,35
2. Самостоятельная работа (СРС)	**57,65**	**57,65**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям)	51,65	51,65
Подготовка к зачету с оценкой	6	6
Вид промежуточного контроля:	Зачет	

*** в том числе практическая подготовка (см. учебный план)**

4.2 Содержание дисциплины

Таблица 3

Тематический план учебной дисциплины

Наименование разделов и тем дисциплин (укрупнёно)	**Всего**	**Аудиторная работа**			**Внеаудиторная работа СР**
		Л	**ПЗ всего/***	**ПКР всего/***	
Тема 1 Место и роль аналитических инструментов в системе обеспечении информационной безопасности организации	13	2	4		7
Тема 2 Правовое обеспечение информационной безопасности	13	2	4		7
Тема 3 Объектно-ориентированный подход к информационной безопасности. Физическая защита объектов. Концепция построения систем защиты.	13	2	4		7
Тема 4 Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	13	2	4		7
Тема 5 Уровни информационной безопасности	13	2	4		7
Тема 6 Аналитические инструменты управления рисками информационной безопасности	13	2	4		7

Наименование разделов и тем дисциплин (укрупнёно)	Всего	Аудиторная работа			Внеаудиторная работа СР
		Л	ПЗ всего/*	ПКР всего/*	
Тема 7 Вредоносное программное обеспечение	16	2	6/2		8
Тема 8. Организация средств защиты информации	13,65	2	4/2		7,65
Контактная работа на промежуточном контроле (КРА)	**0,35**			**0,35**	
Итого по дисциплине	**108**	**16**	**34/4**	**0,35**	**57,65**

*** в том числе практическая подготовка (см. учебный план)**

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, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

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, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

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, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

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, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

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, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

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, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

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 программного обеспечения. Полиморфизм и обфускация. Борьба с антивирусами. Направления самозащиты. Типы антивирусов. Правила обработки информации. Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации финансовой информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

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, Miro, Zoom, Trello, 1С: ERP, Битрикс24.

4.3 Лекции/практические занятия

Таблица 4

Содержание лекций/практических занятий и контрольные мероприятия

№ п/п	№ раздела	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов/*
1.	Тема 1 Место и роль аналитических инструменто	Лекция №1 Место и роль аналитических инструментов в системе обеспечении информационной безопасности организации	Пкос-2.1; Пкос-2.2; Пкос-2.3		2

№ п/п	№ раздела	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов/*
	в в системе обеспечении информационной безопасности организации	Практическая работа №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	4
2.	Тема 2. Правовое обеспечение информационной безопасности	Лекция №2 Правовое обеспечение информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3		2
		Практическая работа №2 Правовое обеспечение информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	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		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	защита лабораторной работы	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		2
		Практическая работа №4 Основные определения и критерии классификации угроз. Оценочные стандарты и технические спецификации	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	4
5.	Тема 5. Уровни информационной безопасности организаций	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	Лекция №6 Аналитические инструменты управления рисками информационной безопасности	Пкос-2.1; Пкос-2.2; Пкос-2.3		2

№ п/п	№ раздела	№ и название лекций/ практических занятий	Формируемые компетенции	Вид контрольного мероприятия	Кол-во часов/*
	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	4
7.	Тема 7 Вредоносное программное обеспечение	Лекция №7 Вредоносное программное обеспечение	Пкос-2.1; Пкос-2.2; Пкос-2.3		2
		Практическая работа №7 Вредоносное программное обеспечение	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы	6/2
8.	Тема 8. Организация средств защиты информации	Лекция №8 Организация средств защиты информации	Пкос-2.1; Пкос-2.2; Пкос-2.3		2
		Практическая работа №8 Организация средств защиты информации	Пкос-2.1; Пкос-2.2; Пкос-2.3	защита практической работы тестирование	4/2

* в том числе практическая подготовка

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

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

№ п/п	№ раздела темы	Перечень рассматриваемых вопросов для самостоятельного изучения
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? ПСК-3 (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
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, пред ставляющими 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 вычис лительной 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

Типовые лабораторные задания по практике дисциплины «Аналитические инструменты обеспечения информационной безопасности»

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 (Пкос-2.1; Пкос-2.2; Пкос-2.3)
2. Информационная база для проведения аналитических процедур (Пкос-2.1; Пкос-2.2; Пкос-2.3)
3. Организационное обеспечение информационной безопасности как составная часть системы комплексного противодействия информационным угрозам (Пкос-2.1; Пкос-2.2; Пкос-2.3)
4. Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране (Пкос-2.1; Пкос-2.2; Пкос-2.3)
5. Основные принципы построения организационного обеспечения защиты информации и предъявляемые к ней требования (Пкос-2.1; Пкос-2.2; Пкос-2.3)
6. Основные цели и задачи организационного обеспечения информационной безопасности на предприятии (Пкос-2.1; Пкос-2.2; Пкос-2.3)
7. Объекты и субъекты организационного обеспечения защиты информации коммуникативного процесса (Пкос-2.1; Пкос-2.2; Пкос-2.3)
8. Угрозы информационной безопасности. Виды угроз. Организационные меры противодействия различным видам угроз (Пкос-2.1; Пкос-2.2; Пкос-2.3)
9. Случайные и преднамеренные угрозы. Меры организационного противодействия случайным и преднамеренным угрозам (Пкос-2.1; Пкос-2.2; Пкос-2.3)
10. Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ (Пкос-2.1; Пкос-2.2; Пкос-2.3)
11. Классификация каналов утечки информации относительно возможных действий нарушителя информационной безопасности (Пкос-2.1; Пкос-2.2; Пкос-2.3)
12. Содержание аналитических документов, необходимых для разработки «Политики информационной безопасности предприятия» (Пкос-2.1; Пкос-2.2; Пкос-2.3)
13. Структура и содержание документа «Политика информационной безопасности предприятия» (Пкос-2.1; Пкос-2.2; Пкос-2.3)
14. Служба информационной безопасности предприятия. Состав, цели и задачи службы информационной безопасности предприятия (Пкос-2.1; Пкос-2.2; Пкос-2.3)
15. Концепция информационной безопасности предприятия. Цели и задачи предприятия в обеспечении информационной безопасности при взаимодействии с внешними и внутренними субъектами информационного обмена (Пкос-2.1; Пкос-2.2; Пкос-2.3)

16. Роль стандартов и требований по информационной безопасности предприятия в формировании «Политики информационной безопасности предприятия» (Пкос-2.1; Пкос-2.2; Пкос-2.3)

17. Процедуры и методы информационной безопасности предприятия как составляющие «Политики информационной безопасности предприятия». Профили защиты (Пкос-2.1; Пкос-2.2; Пкос-2.3)

18. Права и обязанности руководящего состава и сотрудников службы информационной безопасности. Роль служебных комиссий и «кризисных групп» в обеспечении информационной безопасности (Пкос-2.1; Пкос-2.2; Пкос-2.3)

19. Порядок установления режима конфиденциальности информации. Перечень сведений, относимых к конфиденциальной информации и не подлежащих засекречиванию (Пкос-2.1; Пкос-2.2; Пкос-2.3)

20. Организация конфиденциального делопроизводства (Пкос-2.1; Пкос-2.2; Пкос-2.3)

21. Общие обязанности сотрудников по неразглашению конфиденциальной информации (Пкос-2.1; Пкос-2.2; Пкос-2.3)

22. Организация доступа и допуска сотрудников к конфиденциальной информации (Пкос-2.1; Пкос-2.2; Пкос-2.3)

23. Организация доступа к информационным системам, обрабатывающим конфиденциальную информацию. Матричный и мандатный подходы к проблемам разграничения доступа (Пкос-2.1; Пкос-2.2; Пкос-2.3)

24. Порядок обеспечения сохранности конфиденциальной информации при постоянном или временном прекращении пользователем доступа к конфиденциальному информационному ресурсу (Пкос-2.1; Пкос-2.2; Пкос-2.3)

25. Требования, предъявляемые к претендентам на работу с конфиденциальной информацией и к претендентам на должность службу информационной безопасности (Пкос-2.1; Пкос-2.2; Пкос-2.3)

26. Кадровая политика предприятия. Возможные источники пополнения предприятия кадрами для работы с конфиденциальной информацией (Пкос-2.1; Пкос-2.2; Пкос-2.3)

27. Порядок организации и проведения конкурсов на замещения вакантных должностей, связанных с безопасностью информации (Пкос-2.1; Пкос-2.2; Пкос-2.3)

28. Методы проверки кандидатов на работу. Отражение вопросов информационной безопасности в трудовых и коллективных договорах (Пкос-2.1; Пкос-2.2; Пкос-2.3)

29. Текущая работа с персоналом, допущенным к конфиденциальной информации. Дисциплинарная ответственность. Меры поощрения и наказания (Пкос-2.1; Пкос-2.2; Пкос-2.3)

30. Методы борьбы с нарушениями информационной безопасности. Порядок завершения текущей работы с сотрудниками, владеющими конфиденциальной информацией при их увольнении (Пкос-2.1; Пкос-2.2; Пкос-2.3)

31. Организация служебного расследования по фактам утечки конфиденциальной информации. Порядок проведения служебного расследования по фактам утраты секретных документов и разглашения конфиденциальной информации (Пкос-2.1; Пкос-2.2; Пкос-2.3)

32. Сложные инциденты. Порядок организации служебного расследования в случаях возникновения сложных инцидентов (Пкос-2.1; Пкос-2.2; Пкос-2.3)

33. Организация охраны объектов информатизации. Составные элементы системы охраны. Требования к охранникам и их обязанностям (Пкос-2.1; Пкос-2.2; Пкос-2.3)

34. Организация режима охраны объекта. Принципы охраны. Факторы, влияющие на выбор приёмов и средств охраны (Пкос-2.1; Пкос-2.2; Пкос-2.3)

35. Организация внутриобъектового и пропускного режимов на объектах информатизации. Цели организации внутриобъктового режима (Пкос-2.1; Пкос-2.2; Пкос-2.3)

36. Зона режимности предприятия. Требования к введению внутриобъктового режима (Пкос-2.1; Пкос-2.2; Пкос-2.3)

37. Организация пропускного режима. Типы пропусков. Учёт пропускных документов (Пкос-2.1; Пкос-2.2; Пкос-2.3)

38. Атрибутивный и биометрический способы идентификации сотрудников. Их преимущества и недостатки (Пкос-2.1; Пкос-2.2; Пкос-2.3)

39. Порядок соблюдения объектового режима при работе с представителями сторонних организаций (Пкос-2.1; Пкос-2.2; Пкос-2.3)

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 помещений (Пкос-2.1; Пкос-2.2; Пкос-2.3)

41. Аттестация помещений, в которых обрабатывается конфиденциальная информация. Этапы проведения аттестации. Технический паспорт на помещение и аттестат соответствия (Пкос-2.1; Пкос-2.2; Пкос-2.3)

42. Порядок организации работ по созданию и эксплуатации объектов информатизации и средств защиты информации (СЗИ), определяемый СТР К. Стадии создания объекты информации (Пкос-2.1; Пкос-2.2; Пкос-2.3)

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 (Пкос-2.1; Пкос-2.2; Пкос-2.3)

44. Порядок защиты информации в СУБД. Защита информации в локальных вычислительных сетях и при выходе в сети общего пользования (Пкос-2.1; Пкос-2.2; Пкос-2.3)

45. Организация защиты информации при взаимодействии со сторонниками организациями. Порядок отбора и подготовки информации к оглашению. Отражение вопросов защиты информации при подготовке договоров (Пкос-2.1; Пкос-2.2; Пкос-2.3)

46. Обеспечение защиты информации при ведении переговоров и при приеме в организации сторонних организаций и посетителей. Особенности обеспечения безопасности информации при приеме иностранных делегаций (Пкос-2.1; Пкос-2.2; Пкос-2.3)

47. Роль информационно-аналитичной работы как составной части организационных методов защиты информации. Основные показатели качества ин-

формации. Методы прогнозирования и верификации (Пкос-2.1; Пкос-2.2; Пкос-2.3)

48. Контроль функционирования системы организационной защиты информации. Формы контроля (Пкос-2.1; Пкос-2.2; Пкос-2.3)

49. Аудит информационной безопасности. Формы аудита. Особенности аудита автоматизированных информационных систем (Пкос-2.1; Пкос-2.2; Пкос-2.3)

50. Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций. Требования пожарной безопасности к объектам информатизации (Пкос-2.1; Пкос-2.2; Пкос-2.3)

51. Меры по охране конфиденциальности информации (Пкос-2.1; Пкос-2.2; Пкос-2.3)

52. Информационное обеспечение аналитических инструментов обеспечения информационной безопасности (Проведение совещаний при помощи Zoom, обмен информацией посредством системы Google –документов, Outlook, Power Point) (Пкос-2.1; Пкос-2.2; Пкос-2.3)

53. Применение в коммуникационном процессе для ускорения передачи, обработки и интерпретации информации программные продукты Excel, Word, Outlook, Power Point, Project Expert, Miro, Zoom, Trello, 1С: ERP, Битрикс24 (Пкос-2.1; Пкос-2.2; Пкос-2.3)

54. Инструменты моделирования и оптимизации решений Project Expert. TABLEAU, Power Point для формирования объективного акта ревизии (Пкос-2.1; Пкос-2.2; Пкос-2.3)

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

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов (табл. 7). Максимальное количество баллов по текущему контролю – 108 баллов.

Таблица 7

Шкала оценивания	Оценка
92-108	Отлично
77-91	Хорошо
65-76	Удовлетворительно
0-64	Неудовлетворительно

В основу балльно-рейтинговой системы (БРС) положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего, промежуточного контроля и промежуточной аттестации знаний. При общей сумме баллов по результатам текущего контроля менее 65 баллов (табл. 8), студенту выставляется оценка «неудовлетворительно».

Ликвидация студентами текущей задолженности осуществляется путем

предоставления конспектов по темам лекций и практических занятий по курсу. Студенту может быть выставлена итоговая оценка по дисциплине на основе набранных баллов по текущему контролю, если студент набрал свыше 64 баллов, если студент не претендует на более высокую оценку. Если он претендует на более высокую оценку, то он отвечает на два вопроса из перечня вопросов к зачету с оценкой. Каждый вопрос оценивается по 10 балльной шкале.

Максимальное количество по промежуточной аттестации – 20

Таблица 9

Общее количество баллов для оценки промежуточного контроля

Максимальная сумма баллов	Зачет с оценкой			
	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
20	0-11	12-14	15-17	18-20

Если по результатам промежуточного контроля студент набирает менее 5 баллов, ему выставляется оценка «неудовлетворительно». Пересдача экзамена осуществляется в соответствии с Положением о промежуточной аттестации студентов в Университете.

Таблица 10

Критерии оценивания результатов обучения

Оценка	**Критерии оценивания**
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы; демонстрирует возможности интернет-ресурсов и программных продуктов при решении профессиональных задач (Консультант, Гарант, официальные сайты министерств и ведомств, Nalog.ru, CRM, ERP системы, Бизнес-навигатор МСП); владеет навыками поиска информации посредством электронных ресурсов (Яндекс, Mail), официальных сайтов различных ведомств; навыками расчёта влияния различных факторов на размер прибыли, используя программу Statistica, осуществлять расчет показателей экономической эффективности проекта с использованием программных продуктов Project Expert, Бизнес-конструктор, Бизнес-навигатор МСП, осуществлять обмен информацией при осуществлении финансовых проверок с применением системы Google, Miro с целью принятия экономически обоснованных управленческих решений при осуществлении ревизии, владения навыками распределения задач в системе Битрикс24, навыками визуализации данных в процессе ревизии с применением TABLEAU; умения применять в коммуникационном процессе для ускорения процесса передачи, обработки и интерпретации финансовой информации такие программные продукты, как Excel, Word, Outlook, Power Point, Project Expert, Miro, Zoom, Trello,1 С: ERP. **Компетенции**, закреплённые за дисциплиной, **сформированы на уровне – высокий**.
Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в ос-

	новном сформировал практические навыки; демонстрирует возможности интернет-ресурсов и программных продуктов при решении профессиональных задач (Консультант, Гарант, официальные сайты мини-стерств и ведомств, Nalog.ru, CRM, ERP системы, Бизнес-навигатор МСП); владеет навыками поиска информации посредством электронных ресурсов (Яндекс, Mail), официальных сайтов различных ведомств; навыками расчёта влияния различных факторов на размер прибыли, используя программу Statistica, осуществлять расчет показателей экономической эффективности проекта с использованием программных продуктов Project Expert, Бизнес-конструктор, Бизнес-навигатор МСП, осуществлять обмен информацией при осуществлении финансовых проверок с применением системы Google, Miro с целью принятия экономически обоснованных управленческих решений при осуществлении ревизии, владения навыками распределения задач в системе Битрикс24, навыками визуализации данных в процессе ревизии с применением TABLEAU. **Компетенции**, закреплённые за дисциплиной, **сформированы на уровне – хороший (средний)**.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы; демонстрирует возможности интернет-ресурсов и программных продуктов при решении профессиональных задач (Консультант, Гарант, официальные сайты министерств и ведомств, Nalog.ru, CRM, ERP системы, Бизнес-навигатор МСП); владеет навыками поиска информации посредством электронных ресурсов (Яндекс, Mail), официальных сайтов различных ведомств. **Компетенции**, закреплённые за дисциплиной, **сформированы на уровне – достаточный**.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы; студент не владеет возможностями интернет-ресурсов и программных продуктов при решении профессиональных задач (Консультант, Гарант, официальные сайты мини-стерств и ведомств, Nalog.ru, CRM, ERP системы, Бизнес-навигатор МСП); не владеет навыками поиска информации посредством электронных ресурсов (Яндекс, Mail), официальных сайтов различных ведомств; не имеет навыков расчёта влияния различных факторов на размер прибыли, используя программу Statistica, не владеет навыками распределения задач в системе Битрикс24, не владеет навыками визуализации данных в процессе ревизии с применением TABLEAU; не умеет применять в коммуникационном процессе для ускорения процесса передачи, обработки и интерпретации финансовой информации такие программные продукты, как Excel, Word, Outlook, Power Point, Project Expert, Miro, Zoom, Trello,1 С: ERP. **Компетенции**, закреплённые за дисциплиной, **не сформированы**.

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 (дата обращения: 07.10.2022).

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 (дата обращения: 07.10.2022).

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 (дата обращения: 07.10.2022).

2. Организационное и правовое обеспечение информационной безопасности : 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 (дата обращения: 07.10.2022).

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 (дата обращения: 29.09.2022).

7.3 Нормативные правовые акты

1. Конституция Российской Федерации, 1993 г. (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 05.02.2014, от 21.07.2014 №11-ФКЗ).

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 (ред. от 29.12.2015) и часть 2 от 05.08.2000 №117-ФЗ (ред. от 29.12.2015).

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.

7. Федеральный закон от 7 февраля 2011 г. №3-ФЗ «О полиции» (в ред. от 21.07.2014 г.).

8. Федеральный закон «О бухгалтерском учете» от 06 декабря 2011 г. №402-ФЗ (в ред. от 28.12.2013 г.).

9. Федеральный закон от 12 августа 1995 №144-ФЗ «Об оперативно-розыскной деятельности» (в ред. от 21.12.2013 г.).

10. Федеральный закон от 26 декабря 1995 №208-ФЗ «Об акционерных обществах» (в ред. от 21.07.2014 г.).

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. . Правительство Российской Федерации. – Открытый доступ. – Режим доступа к материалам: http://government.ru.
2. Министерство сельского хозяйства Российской Федерации. – Открытый доступ. – Режим доступа к материалам: http://mcx.ru
3. Министерство экономического развития Российской Федерации. – Открытый доступ. – Режим доступа к материалам: http://economy.gov.ru.
4. Федеральная служба безопасности РФ. – Открытый доступ. – Режим доступа к материалам: http://fsb.ru.
5. Министерство внутренних дел Российской Федерации. – Открытый доступ. – Режим доступа к материалам: http://мвд.рф.
6. Электронная библиотека бесплатных электронных книг по бизнесу, финансам, экономике и смежным темам. – Открытый доступ. – Режим доступа к материалам: http://www.finbook.biz.
7. Библиотека экономической и управленческой литературы. – Открытый доступ. – Режим доступа к материалам: http://eup.ru.
8. Библиотека экономических журналов на английском языке. – Открытый доступ. – Режим доступа к материалам: http://www.oswego.edu/~economic/journals.htm

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Для освоения дисциплины рекомендуются следующие сайты информационно-телекоммуникационной сети «Интернет»:

- официальный сайт университета: https://www.timacad.ru/
- Федеральная служба государственной статистики. – Режим доступа: http://www.gks.ru
- Битрикс24. Официальный сайт. Режим доступа: https://www.bitrix24.ru/whatisthis/ – https://www.tableau.com/products
- Бизнес-портал Бизнес-навигатор МСП. Электронный ресурс. Режим доступа https://smbn.ru/
- Справочная правовая система «КонсультантПлюс» Режим доступа www.consultant.ru

- Справочная правовая система «Гарант» Режим доступа www.garant.ru

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия проводятся в аудиториях, оборудованных мультимедийными средствами.

Особых требований к мультимедийному оборудованию нет.

Требований к программному обеспечению учебного процесса дисциплины «Аналитические инструменты обеспечения информационной безопасности»: Google-документы, Zoom, Miro, Яндекс, Mail, Битрикс24.

Таблица 11

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
1	2
Учебная аудитория (1 учебный корпус, 502 аудитория)	Средства мультимедиа
Учебная аудитория (15 учебный корпус, 226 аудитория)	Средства мультимедиа
Учебная аудитория (12 учебный корпус, 7 аудитория)	Компьютерный класс на 26 компьютеров
Учебная аудитория (12 учебный корпус, 12 аудитория)	Компьютерный класс на 22 компьютера
Учебная аудитория (12 учебный корпус, 13 аудитория)	Компьютерный класс на 26 компьютеров
Учебная аудитория (15 учебный корпус, 102 аудитория)	Компьютерный класс на 21 компьютер
Учебная аудитория (15 учебный корпус, 113 аудитория)	Компьютерный класс на 20 компьютеров
Учебная аудитория (15 учебный корпус, 114 аудитория)	Компьютерный класс на 17 компьютеров
Учебная аудитория (15 учебный корпус, 110 аудитория)	Компьютерный класс на 18 компьютеров
Учебная аудитория (15 учебный корпус, 118 аудитория)	Компьютерный класс на 18 компьютеров
ЦНБ имени Н.И. Железнова	Читальные залы
Помещения для самостоятельной работы студентов: Корпус 2, аудитория 321;	1.Столы – 7 шт. (инв. номер: 632634, 625631, 591194) 2.Стулья – 21 шт. (инв. номер 558590) 3.Проектор NEC NP 200 (G) – 1 шт. (инв. номер 210134000002612) 4. Ноутбук HP 6720s – 1шт. (инв. номер 210134000006213) 5. Маркерная доска – 1 шт. 6. Компьютеры для индивидуальной работы

11. Методические рекомендации студентам по освоению дисциплины

Образовательный процесс по дисциплине «Аналитические инструменты обеспечения информационной безопасности» организован в форме учебных занятий (контактная работа (аудиторной и внеаудиторной) обучающихся с преподавателем и самостоятельная работа обучающихся). Учебные занятия (в том числе по реализации практической подготовки) представлены следующими видами, включая учебные занятия, направленные на практическую подготовку обучающихся и проведение текущего контроля успеваемости: лекции, практические занятия, иные учебные занятия, предусматривающие индивидуальную работу преподавателя с обучающимся, самостоятельная работа обучающихся.

На учебных занятиях обучающиеся выполняют запланированные настоящей программой отдельные виды учебных работ, в том числе отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Виды и формы отработки пропущенных занятий

Студент, пропустивший лекцию, обязан сдать реферат в виде блок-схемы по основным вопросам темы лекции.

Студент, пропустивший практические занятия, обязан сдать письменный отчет по проблемной ситуации, рассматриваемой на практическом занятии, и пройти мероприятия текущего контроля.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

Изучаемые в рамках дисциплины «Аналитические инструменты обеспечения информационной безопасности» темы взаимосвязаны между собой и с материалами ранее изученных дисциплин. Следовательно, преподавателю целесообразно обращать внимание студентов на системность изучаемого материала в аспектах специализации «Экономико-правовое обеспечение экономической безопасности».

Для облегчения студентам восприятия материала по дисциплине «Аналитические инструменты обеспечения информационной безопасности» много времени уделяется активным и интерактивным образовательным технологиям, что способствует преодолению пассивности обучающихся.

Программу разработали:

к.э.н., доцент Катков Ю.Н.

к.э.н., доцент Каткова Е.А.

РЕЦЕНЗИЯ
на рабочую программу дисциплины
Б1.В.10.06 Аналитические инструменты обеспечения информационной безопасности
ОПОП ВО по специальности 38.05.01 Экономическая безопасность, специализации
Экономико-правовое обеспечение экономической безопасности
(квалификация выпускника – экономист)

Хоружий Людмилой Ивановной, директором института экономики и управления АПК, профессором кафедры бухгалтерского учета и налогообложения ФГБОУ ВО «РГАУ-МСХА имени К.А. Тимирязева», доктором экономических наук, профессором (далее по тексту рецензент), проведено рецензирование рабочей программы дисциплины «Аналитические инструменты обеспечения информационной безопасности» ОПОП ВО специальности 38.05.01 Экономическая безопасность, специализации Экономико-правовое обеспечение экономической безопасности (квалификация выпускника – экономист), разработанной в ФГБОУ ВО «РГАУ-МСХА имени К.А. Тимирязева», на кафедре экономической безопасности, анализа и аудита (разработчики Катков Ю.Н., к.э.н., доцент и Каткова Е.А., к.э.н., доцент).

Рассмотрев представленные на рецензию материалы, рецензент пришел к следующим выводам:

1. Предъявленная рабочая программа дисциплины «Аналитические инструменты обеспечения информационной безопасности» (далее по тексту Программа) *соответствует* требованиям ФГОС ВО по специальности 38.05.01 Экономическая безопасность. Программа *содержит* все основные разделы, *соответствует* требованиям к нормативно-методическим документам.

2. Представленная в Программе *актуальность* учебной дисциплины в рамках реализации ОПОП ВО *не подлежит сомнению* – дисциплина относится к части, формируемую участниками образовательных отношений блока Б1.В.

3. Представленные в Программе ***цели*** дисциплины *соответствуют* требованиям ФГОС ВО по специальности 38.05.01 Экономическая безопасность.

4. В соответствии с Программой за дисциплиной «Аналитические инструменты обеспечения информационной безопасности» закреплены 3 компетенции. Дисциплина «Аналитические инструменты обеспечения информационной безопасности» и представленная Программа *способна реализовать* их в объявленных требованиях.

5. *Результаты обучения*, представленные в Программе в категориях знать, уметь, владеть *соответствуют* специфике и содержанию дисциплины и *демонстрируют возможность* получения заявленных результатов.

6. Общая трудоёмкость дисциплины «Аналитические инструменты обеспечения информационной безопасности» составляет 3 зачётные единицы (108 часа), что позволяет освоить дисциплину в рамках необходимой компетентности выпускников.

7. Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин *соответствует* действительности. Дисциплина «Аналитические инструменты обеспечения информационной безопасности» взаимосвязана с другими дисциплинами ОПОП ВО и Учебного плана по специальности 38.05.01 «Экономическая безопасность» и возможность дублирования в содержании отсутствует. Поскольку дисциплина не предусматривает наличие специальных требований к входным знаниям, умениям и компетенциям студента, хотя может являться предшествующей для специальных, в том числе профессиональных дисциплин, использующих знания в области судебной экономической экспертизы в профессиональной деятельности специалиста по данной специальности.

8. Представленная Программа предполагает использование современных образовательных технологий, используемых при реализации различных видов учебной работы. Формы образовательных технологий *соответствуют* специфике дисциплины.

9. Программа дисциплины предполагает занятия в интерактивной форме.

10. Виды, содержание и трудоёмкость самостоятельной работы студентов, представленные в Программе, *соответствуют* требованиям к подготовке выпускников, содержащимся во ФГОС ВО по специальности 38.05.01 Экономическая безопасность.

11. Представленные и описанные в Программе формы *текущей* оценки знаний (выполнение и защита практических заданий, контрольные работы), *соответствуют* специфике дисциплины и требованиям к выпускникам.

Форма промежуточного контроля знаний студентов, предусмотренная Программой, осуществляется в виде экзамена во 6 семестре, что соответствует требованиям для дисциплин данного объема и Учебному плану.

12. Формы оценки знаний, представленные в Программе, *соответствуют* специфике дисциплины и требованиям к выпускникам.

13. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 2 источника (базовых учебников), дополнительной литературой – 3 наименований, Интернет-ресурсами – 8 источников, информационно-справочные и поисковые системы и соответствует требованиям ФГОС ВО специальности 38.05.01 – Экономическая безопасность.

14. Материально-техническое обеспечение дисциплины *соответствует* специфике дисциплины «Аналитические инструменты обеспечения информационной безопасности» и обеспечивает использование современных образовательных, в том числе интерактивных методов обучения.

15. Методические рекомендации студентам и методические рекомендации преподавателям по организации обучения по дисциплине дают представление о специфике обучения по дисциплине «Аналитические инструменты обеспечения информационной безопасности».

ОБЩИЕ ВЫВОДЫ

На основании вышеизложенного можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Аналитические инструменты обеспечения информационной безопасности» ОПОП ВО по специальности 38.05.01 Экономическая безопасность специализации Экономико-правовое обеспечение экономической безопасности (квалификация выпускника – экономист), разработанная Катковым Ю.Н. и Катковой Е.А. соответствует требованиям ФГОС ВО, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент: Рецензент: Хоружий Людмила Ивановна, директор института экономики и управления АПК, профессор кафедры бухгалтерского учета и налогообложения ФГБОУ ВО «Российский государственный аграрный университет - МСХА имени К.А. Тимирязева», доктор экономических наук

«01» июня 2022 г.