

Документы Федерального государственного автономного образовательного учреждения высшего образования
Информация о владельце: "Самарский государственный экономический университет"
ФИО: Кандрашина Елена Александровна
Должность: И.о. ректора ФГАОУ ВО «Самарский государственный экономический университет»
Дата подписания: 08.07.2026 10:29:16
Уникальный программный ключ:
2db64eb9605ce27edd3b8e8fdd32c70e0674ddd2

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ
ОБЩЕСТВЕ»**

Уровень высшего образования: специалитет

Специальность: 38.05.01 Экономическая безопасность

Направленность (профиль)подготовки: Экономическая безопасность

Квалификация (степень) выпускника: экономист

Формы обучения: очная, очно-заочная

Год набора (приема на обучение): 2026

Срок получения образования: Очная форма обучения – 5 лет
 Очно-заочная форма обучения – 5 лет 6 месяца(-ев)

Объем: в зачетных единицах: 4 з.е.
 в академических часах: 144 ак.ч.

г. Самара, 2026

Разработчики:

Кандидат экономических наук Татаровская Т. Е.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по специальности 38.05.01 Экономическая безопасность, утвержденного приказом Минобрнауки от 14.04.2021 № 293, с учетом трудовых функций профессиональных стандартов: "Специалист по управлению рисками", утвержден приказом Минтруда России от 18.04.2025 № 264н; "Специалист по финансовому мониторингу (в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма)", утвержден приказом Минтруда России от 24.07.2015 № 512н; "Специалист по конкурентному праву", утвержден приказом Минтруда России от 16.09.2021 № 637н; "Специалист в сфере предупреждения коррупционных правонарушений", утвержден приказом Минтруда России от 08.08.2022 № 472н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Кафедра учета, анализа и экономической безопасности	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Татаровский Ю. А.	Рассмотрено	26.05.2026, № 12

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

Задачи изучения дисциплины:

- Формирование у обучающихся способности осуществлять раскрытие информации о рисках организации в отчетах для внешних пользователей в соответствии с требованиями регуляторов и международными стандартами.;
- Развитие навыков интеграции информации о рисках в отчетность организации с учетом их влияния на достижение стратегических целей и принимаемые управленческие решения.;
- Обучение методам подготовки и представления сведений о рисках экономической безопасности в публичной отчетности, обеспечивающих прозрачность и взаимосвязь с общей стратегией развития организации в условиях цифровой экономики..

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-2 Способен осуществлять раскрытие информации о рисках организации в отчетах для внешних сторон в соответствии с требованиями регуляторов, а также во взаимосвязи с достижением стратегических целей и принимаемыми стратегическими решениями

ПК-2.1 Формирует, анализирует и интерпретирует информацию, необходимую для принятия решений по обеспечению экономической безопасности субъектов

Знать:

ПК-2.1/Зн1 Методы формирования, анализа и интерпретации информации о рисках и угрозах экономической безопасности субъектов в условиях цифрового общества.

Уметь:

ПК-2.1/Ум1 Формировать, анализировать и интерпретировать информацию, необходимую для принятия решений по обеспечению экономической безопасности организации.

Владеть:

ПК-2.1/Нв1 Навыками сбора, обработки и интерпретации данных о рисках экономической безопасности для подготовки управленческих решений.

ПК-2.2 Использует полученные сведения для принятия решений по предупреждению, локализации и нейтрализации угроз экономической безопасности для достижения стратегических целей

Знать:

ПК-2.2/Зн1 Механизмы и инструменты использования информации о рисках для предупреждения, локализации и нейтрализации угроз экономической безопасности.

Уметь:

ПК-2.2/Ум1 Использовать проанализированные сведения для принятия решений по предотвращению и нейтрализации угроз экономической безопасности в целях достижения стратегических целей организации.

Владеть:

ПК-2.2/Нв1 Навыками применения аналитической информации при разработке и реализации мер по предупреждению, локализации и нейтрализации угроз экономической безопасности в цифровой среде.

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Обеспечение экономической безопасности в цифровом обществе» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): Очная форма обучения - 9, Очно-заочная форма обучения - 9.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ПК-2 - Способен осуществлять раскрытие информации о рисках организации в отчетах для внешних сторон в соответствии с требованиями регуляторов, а также во взаимосвязи с достижением стратегических целей и принимаемыми стратегическими решениями		
ПК-2.1 Формирует, анализирует и интерпретирует информацию, необходимую для принятия решений по обеспечению экономической безопасности субъектов	Бухгалтерский управленческий учет, Информационные системы в экономике, Лабораторный практикум 1С, Обеспечение экономической безопасности государственных закупок, Стратегический анализ, Экономическая безопасность в нефтяных и строительных организациях, Экономическая безопасность в страховых и кредитных организациях, Экономическая безопасность предприятий АПК, Электронные носители отчетности	Обеспечение экономической безопасности государственных закупок, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика, Стратегический анализ, Экономическая безопасность в страховых и кредитных организациях, Экономическая безопасность предприятий АПК
ПК-2.2 Использует полученные сведения для принятия решений по предупреждению, локализации и нейтрализации угроз экономической безопасности для достижения стратегических целей	Информационные системы в экономике, Комплексный экономический анализ финансово-хозяйственной деятельности, Лабораторный практикум 1С, Обеспечение экономической безопасности государственных закупок, Стратегический анализ, Экономическая безопасность в государственных и муниципальных учреждениях, Электронные носители отчетности	Обеспечение экономической безопасности государственных закупок, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика, Стратегический анализ, Экономическая безопасность в государственных и муниципальных учреждениях

4. Объем дисциплины (модуля) и виды учебной работы

Очная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лекционные занятия (часы)	Практические занятия (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Девятый семестр	144	4	36	18	18	0,15	89,85	Зачет
Всего	144	4	36	18	18	0,15	89,85	18

Очно-заочная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Лекционные занятия (часы)	Практические занятия (часы)	Индивидуальная контактная работа (часы)	Самостоятельная работа (часы)	Промежуточная аттестация
Девятый семестр	144	4	4	2	2	0,15	121,85	Зачет
Всего	144	4	4	2	2	0,15	121,85	18

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий
(часы промежуточной аттестации не указываются)

Очная форма обучения

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа
Раздел 1. Теоретические основы обеспечения экономической безопасности в цифровом обществе	56	8	8	40
Тема 1.1. Понятие цифрового общества. Особенности цифровизации в России на современном этапе	14	2	2	10

Тема 1.2. Цель и задачи системы экономической безопасности в современных условиях	14	2	2	10
Тема 1.3. Современные угрозы, связанные с цифровизацией	14	2	2	10
Тема 1.4. Современные угрозы экономической безопасности в цифровом обществе	14	2	2	10
Раздел 2. Методические основы обеспечения экономической безопасности в цифровом обществе	69,85	10	10	49,85
Тема 2.1. Проблемы экономической безопасности цифрового общества и направления их решения	14	2	2	10
Тема 2.2. Модель экономической безопасности в цифровом обществе в современных условиях	14	2	2	10
Тема 2.3. Методика обеспечения экономической безопасности в цифровом обществе	14	2	2	10
Тема 2.4. Инструменты управления рисками в области обеспечения экономической безопасности в цифровом обществе	14	2	2	10
Тема 2.5. Мониторинг обеспечения безопасности в цифровом обществе	13,85	2	2	9,85

Очно-заочная форма обучения

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа
Раздел 1. Теоретические основы обеспечения экономической безопасности в цифровом обществе	62	1	1	60
Тема 1.1. Понятие цифрового общества. Особенности цифровизации в России на современном этапе	15,5	0,5		15

Тема 1.2. Цель и задачи системы экономической безопасности в современных условиях	15,5		0,5	15
Тема 1.3. Современные угрозы, связанные с цифровизацией	15,5	0,5		15
Тема 1.4. Современные угрозы экономической безопасности в цифровом обществе	15,5		0,5	15
Раздел 2. Методические основы обеспечения экономической безопасности в цифровом обществе	63,85	1	1	61,85
Тема 2.1. Проблемы экономической безопасности цифрового общества и направления их решения	15,5	0,5		15
Тема 2.2. Модель экономической безопасности в цифровом обществе в современных условиях	15,5		0,5	15
Тема 2.3. Методика обеспечения экономической безопасности в цифровом обществе	15,5	0,5		15
Тема 2.4. Инструменты управления рисками в области обеспечения экономической безопасности в цифровом обществе	17,35		0,5	16,85
Тема 2.5. Мониторинг обеспечения безопасности в цифровом обществе				

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестирование Упражнение на заполнение пробела
Промежуточная аттестация	Зачет

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Теоретические основы обеспечения экономической безопасности в цифровом обществе	Тестирование	Зачет
2	Методические основы обеспечения экономической безопасности в цифровом обществе	Упражнение на заполнение пробела	Зачет

6. Оценочные материалы текущего контроля

1. Теоретические основы обеспечения экономической безопасности в цифровом обществе Тестирование

№ п/п	Содержание вопроса		Компетенция
	Правильный ответ (ключ ответа)		
1	<p>Выберите один правильный ответ</p> <p>К правовым методам, обеспечивающим информационную безопасность, относятся:</p> <ol style="list-style-type: none"> 1. разработка аппаратных средств обеспечения правовых данных 2. разработка и установка во всех компьютерных правовых сетях журналов учета действий 3. разработка и конкретизация правовых нормативных актов обеспечения безопасности 		ПК-2
	Ответ:	3	
2	<p>Выберите один правильный ответ</p> <p>Основными источниками угроз финансовой кибербезопасности являются:</p> <ol style="list-style-type: none"> 1. хищение жестких дисков, подключение к сети, инсайдерство 2. перехват данных, хищение данных, изменение архитектуры системы 3. хищение данных, подкуп системных администраторов, нарушение регламента работы 		ПК-2
	Ответ:	3	
3	<p>Выберите один правильный ответ</p> <p>Виды информационной безопасности:</p> <ol style="list-style-type: none"> 1. персональная, корпоративная, государственная 2. клиентская, серверная, сетевая 3. локальная, глобальная, смешанная 		ПК-2
	Ответ:	1	
4	<p>Выберите один правильный ответ</p> <p>Цели финансовой кибербезопасности – своевременное обнаружение, предупреждение:</p> <ol style="list-style-type: none"> 1. несанкционированного доступа, воздействия в сети 2. инсайдерства в организации 3. чрезвычайных ситуаций 		ПК-2
	Ответ:	1	
5	<p>Выберите один правильный ответ</p> <p>Основные объекты информационной безопасности:</p> <ol style="list-style-type: none"> 1. компьютерные сети, базы данных 2. информационные системы, психологическое состояние пользователей 3. бизнес-ориентированные, коммерческие системы 		ПК-2
	Ответ:	1	
6	<p>Установите соответствие</p> <p>Соотнесите виды киберугроз с их характеристиками:</p> <ol style="list-style-type: none"> 1. Фишинг 2. DDoS атаки 3. Программы вымогатели (ransomware) 4. Целевые атаки (APT) <p>А. Вредоносное ПО, блокирующее доступ к системе или данным до выплаты выкупа Б. Массовые рассылки поддельных сообщений с целью получения конфиденциальных данных (логинов, паролей, данных карт) В. Перегрузка серверов запросами с множества устройств для нарушения работы веб ресурсов Г. Длительные и тщательно спланированные атаки на конкретную организацию с целью кражи данных или саботажа</p>		ПК-2
	Ответ:	1 — Б 2 — В 3 — А 4 — Г	
7	<p>Установите соответствие</p> <p>Соотнесите меры обеспечения экономической безопасности с уровнями их применения:</p> <ol style="list-style-type: none"> 1. Разработка национальной стратегии кибербезопасности 2. Внедрение систем обнаружения вторжений (IDS/IPS) 3. Участие в международных соглашениях по борьбе с киберпреступностью 4. Обучение сотрудников правилам кибергигиены 5. Использование сложных паролей и двухфакторной аутентификации <p>А. Уровень предприятия Б. Международный уровень В. Государственный уровень Г. Уровень отдельного пользователя Д. Уровень предприятия и пользователя</p>		ПК-2
	Ответ:	1 — В 2 — А 3 — Б 4 — Г 5 — Д	

8	<p>Установите соответствие</p> <p>Соотнесите нормативно правовые акты РФ с их назначением в сфере экономической безопасности цифрового общества:</p> <ol style="list-style-type: none"> 1. Федеральный закон № 152 ФЗ «О персональных данных» 2. Федеральный закон № 149 ФЗ «Об информации, информационных технологиях и о защите информации» 3. Федеральный закон № 187 ФЗ «О безопасности критической информационной инфраструктуры РФ» 4. Доктрина информационной безопасности РФ (утв. Указом Президента РФ № 646) <p>А. Регулирует создание, применение и защиту криптографических средств защиты информации Б. Устанавливает правила обработки и защиты персональных данных граждан В. Определяет общие принципы регулирования информационных отношений, включая вопросы информационной безопасности Г. Определяет стратегические цели и направления обеспечения безопасности объектов критической информационной инфраструктуры Д. Формулирует стратегические приоритеты и угрозы в сфере информационной безопасности на национальном уровне</p>	ПК-2
	<p>Ответ: 1 — Б 2 — В 3 — Г 4 — Д</p>	
9	<p>Установите правильную последовательность этапов реагирования на киберинцидент в организации Расположите этапы в порядке их выполнения:</p> <ol style="list-style-type: none"> А. Локализация инцидента: изоляция затронутых систем Б. Уведомление заинтересованных сторон В. Выявление и анализ инцидента Г. Устранение последствий Д. Документирование инцидента и подготовка отчёта Е. Мониторинг и контроль 	ПК-2
	<p>Ответ: В → А → Г → Б → Д → Е</p>	
10	<p>Установите правильную последовательность действий при проведении оценки рисков информационной безопасности в организации. Расположите действия в порядке их выполнения:</p> <ol style="list-style-type: none"> А. Идентификация активов Б. Разработка и внедрение мер по снижению рисков В. Оценка угроз и уязвимостей Г. Оценка рисков Д. Переоценка рисков Е. Приоритизация рисков 	ПК-2
	<p>Ответ: А → В → Г → Е → Б → Д</p>	

2. Методические основы обеспечения экономической безопасности в цифровом обществе

Упражнение на заполнение пробела

№ п/п	Содержание вопроса		Компетенция
	Правильный ответ (ключ ответа)		
1	<p>Вставьте пропущенное слово</p> <p>Состояние защищённости национальных экономических интересов от внутренних и внешних угроз в условиях активного использования цифровых технологий, обеспечивающее устойчивое развитие экономики, сохранность данных и бесперебойность цифровых процессов – это ...</p>	ПК-2	
	<p>Ответ: экономическая безопасность в цифровом обществе</p>		
2	<p>Вставьте пропущенное слово</p> <p>Потенциальная возможность нанесения ущерба экономическим интересам субъекта (государства, организации, гражданина) посредством целенаправленных действий в цифровой среде: кибератак, фишинга, DDoS атак, утечки данных и иных вредоносных операций с использованием информационных технологий – это ...</p>	ПК-2	
	<p>Ответ: киберугроза</p>		
3	<p>Вставьте пропущенное слово</p> <p>Комплекс взаимосвязанных цифровых систем, сетей связи, центров обработки данных, программных платформ и сервисов, обеспечивающих функционирование экономики и предоставление цифровых услуг; её надёжность и защищённость критически важны для экономической безопасности – это ...</p>	ПК-2	
	<p>Ответ: критическая информационная инфраструктура</p>		
4	<p>Вставьте пропущенное слово</p> <p>Совокупность правовых, организационных и технических мер, направленных на предотвращение несанкционированного доступа, утечки, искажения или уничтожения информации экономического характера в цифровой среде – это ...</p>	ПК-2	
	<p>Ответ: информационная безопасность</p>		
5	<p>Вставьте пропущенное слово</p> <p>Информационные системы, сети и объекты, нарушение работы которых может привести к серьёзным негативным последствиям для экономики, социальной стабильности и национальной безопасности – это ...</p>	ПК-2	
	<p>Ответ: объекты критической информационной инфраструктуры</p>		

7. Оценочные материалы промежуточной аттестации

Зачет девятый семестр - очная, очно-заочная

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	Дайте развернутый ответ Понятие цифрового общества.		ПК-2
	Ответ:	Цифровое общество — это этап развития информационного общества, характеризующийся масштабной цифровой трансформацией общественных институтов, социальных отношений, экономики, культуры и образования. В таком обществе ключевые процессы — производство, хранение, обработка и передача информации — опираются на цифровые технологии, а взаимодействие между субъектами отношений всё чаще происходит в цифровом формате	
2	Дайте развернутый ответ Особенности цифровизации в России на современном этапе		ПК-2
	Ответ:	Среди особенностей — акцент на импортозамещение в ИТ-сфере (замена иностранного ПО и оборудования на отечественные решения), активное развитие промышленного интернета вещей (IoT), внедрение цифровых технологий в госсектор (электронные госуслуги), а также значительные инвестиции в развитие инфраструктуры 5G и облачных технологий. При этом сохраняются вызовы: цифровое неравенство, дефицит квалифицированных кадров, зависимость от зарубежных технологий в некоторых сегментах и необходимость усиления кибербезопасности.	
3	Дайте развернутый ответ Цель и задачи системы экономической безопасности в современных условиях		ПК-2
	Ответ:	Главная цель — обеспечение устойчивого развития экономики, защита национальных экономических интересов от внутренних и внешних угроз, поддержание конкурентоспособности и инновационного потенциала страны. Задачи включают: формирование эффективной структуры экономики, снижение дефицита бюджета и государственного долга, обеспечение социальной защиты и повышения качества жизни населения, стабилизацию национальной валюты, защиту от кибератак, промышленного шпионажа и других угроз.	
4	Дайте развернутый ответ Современные угрозы, связанные с цифровизацией		ПК-2
	Ответ:	К ним относятся рост числа и сложности кибератак, утечка персональных и корпоративных данных, алгоритмическая дискриминация (необоснованные решения, принимаемые ИИ), цифровой разрыв (неравенство в доступе к технологиям), зависимость от зарубежных технологий, риски, связанные с использованием ИИ (например, «чёрный ящик» — невозможность объяснить решения нейросетей), а также социальные риски, такие как структурная безработица из-за автоматизации.	
5	Дайте развернутый ответ Современные угрозы экономической безопасности в цифровом обществе		ПК-2
	Ответ:	Это могут быть промышленный шпионаж, манипуляции с финансовыми инструментами через цифровые каналы, мошенничество в цифровом пространстве, потеря контроля над критически важными инфраструктурами из-за кибератак, зависимость от иностранных цифровых платформ и технологий, а также риски, связанные с использованием больших данных и ИИ для принятия решений, влияющих на экономику.	
6	Дайте развернутый ответ Мировые тенденции развития технологий big data.		ПК-2
	Ответ:	Среди ключевых трендов — автоматизированное управление метаданными (классификация и каталогизация данных без участия человека), использование синтетических данных для обучения ИИ-моделей, активный мониторинг качества данных, демократизация доступа к аналитическим инструментам через низкокодовые платформы, интеграция ИИ в экосистему Big Data (автономные аналитические платформы, самооптимизирующиеся алгоритмы), а также развитие периферийных вычислений (обработка данных ближе к их источникам).	
7	Дайте развернутый ответ Перспективы использования нейротехнологий и технологий искусственного интеллекта в информационных системах и технологиях управления финансами.		ПК-2
	Ответ:	ИИ может автоматизировать рутинные операции (обработка документов, анализ финансовых отчётов), прогнозировать рыночные тренды, выявлять мошенничество и аномальные транзакции, персонализировать финансовые услуги (например, создавать индивидуальные инвестиционные стратегии), а также оптимизировать управление активами. Нейротехнологии могут применяться для анализа поведенческих данных клиентов и повышения точности предсказаний. Однако есть риски: алгоритмическая предвзятость, проблемы с объяснимостью решений ИИ, угрозы кибербезопасности при централизации данных.	
8	Дайте развернутый ответ Мировые тенденции развития технологии блокчейн.		ПК-2

	<p>Ответ: Наблюдается рост использования смарт-контрактов в различных отраслях (логистика, страхование, управление цепочками поставок), токенизация активов (превращение недвижимости, акций, произведений искусства в цифровые токены), интеграция с ИИ для создания децентрализованных автономных агентов (ДАС), развитие «зеленого» блокчейна (снижение углеродного следа), а также активное внедрение в госуслуги и цифровые валюты (CBDC).</p>	
9	<p>Дайте развернутый ответ Промышленный интернет: направления развития.</p> <p>Ответ: Ключевые направления — интеграция данных систем разного уровня (например, ISA-95 в MES), переход на no-code/low-code-платформы для ускорения цифровизации, цифровая привязка бизнес-процессов к данным с оборудования, замена импортного ПО на российское, дооснащение производств устройствами сбора данных для устранения «слепых зон», отказ от бумажных носителей и Excel в пользу цифровых процессов.</p>	ПК-2
10	<p>Дайте развернутый ответ Перспективы использования технологий виртуальной и дополненной реальности в информационных системах цифровой экономики.</p> <p>Ответ: Эти технологии применяются для бизнес-аналитики и визуализации данных (3D-модели, иммерсивные графики), маркетинга и потребительского опыта (интерактивные презентации продуктов), обучения персонала (симуляции реальных экономических процессов), управления проектами и моделирования бизнес-процессов. В будущем их потенциал будет расти благодаря интеграции с ИИ, развитию 5G и облачных вычислений.</p>	ПК-2

7.1. Уровни овладения

Компетенция: ПК-2 Способен осуществлять раскрытие информации о рисках организации в отчетах для внешних сторон в соответствии с требованиями регуляторов, а также во взаимосвязи с достижением стратегических целей и принимаемыми стратегическими решениями.

Индикатор достижения компетенции: ПК-2.1 Формирует, анализирует и интерпретирует информацию, необходимую для принятия решений по обеспечению экономической безопасности субъектов.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100
Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

Индикатор достижения компетенции: ПК-2.2 Использует полученные сведения для принятия решений по предупреждению, локализации и нейтрализации угроз экономической безопасности для достижения стратегических целей.

Уровень	Характеристика	Оценка в баллах
Повышенный	Достигнуто полное овладение знаниями, умениями и навыками. Студент свободно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	81-100

Базовый	Достигнуто достаточное овладение знаниями, умениями и навыками. Студент уверенно владеет терминологией, умеет применять теоретические знания в различных ситуациях для решения поставленных задач.	61-80
Пороговый	Достигнуто овладение минимально необходимыми знаниями, умениями и навыками. Студент владеет основной терминологией, умеет применять теоретические знания для решения поставленных задач в стандартных ситуациях.	41-60
Ниже порогового	Компетенция не освоена	0-40

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Севрюкова, Е. А. Надзор и контроль в сфере безопасности: учебник для вузов / Е. А. Севрюкова; Е. А. Севрюкова ; под общей редакцией В. И. Каракеяна.. - 2-е изд. - Москва: Юрайт, 2026. - 340 с - 978-5-534-18629-1. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: <https://urait.ru/bcode/582916> (дата обращения: 21.05.2026). - Режим доступа: по подписке
2. Экономическая безопасность: учебник для вузов / Л. П. Гончаренко, Е. В. Баланюк, Л. Л. Баланюк [и др.] - 3-е изд. - Москва: Юрайт, 2026. - 370 с - 978-5-534-17279-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: <https://urait.ru/bcode/583017> (дата обращения: 21.05.2026). - Режим доступа: по подписке
3. Безопасность предпринимательской деятельности: учебник для вузов / В. Л. Шульц, А. В. Юрченко, Н. А. Волобуев, С. К. Кузнецов. - 3-е изд. - Москва: Юрайт, 2026. - 563 с - 978-5-534-18863-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: <https://urait.ru/bcode/587961> (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Кузнецова, Е. Экономическая безопасность: учебник и практикум для вузов / Е. Кузнецова. - 3-е изд. - Москва: Юрайт, 2026. - 338 с - 978-5-534-16876-1. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: <https://urait.ru/bcode/584385> (дата обращения: 21.05.2026). - Режим доступа: по подписке
2. Пименов, Н. А. Управление финансовыми рисками в системе экономической безопасности: учебник и практикум для вузов / Н. А. Пименов. - 3-е изд. - Москва: Юрайт, 2026. - 353 с - 978-5-534-16342-1. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: <https://urait.ru/bcode/582946> (дата обращения: 21.05.2026). - Режим доступа: по подписке
3. Федорова, И. Ю. Финансовый механизм государственных и муниципальных закупок: учебник для вузов / И. Ю. Федорова, А. В. Фрыгин, М. Н. Прокофьев. - 2-е изд. - Москва: Юрайт, 2026. - 235 с - 978-5-534-16600-2. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: <https://urait.ru/bcode/584101> (дата обращения: 21.05.2026). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. <http://www.gov.ru/> - Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия»)
2. <http://pravo.gov.ru/> - Государственная система правовой информации «Официальный интернет-портал правовой информации»

3. <https://www.minfin.ru/ru/> - Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ)

Ресурсы «Интернет»

1. <https://rosstat.gov.ru/> - Федеральная служба государственной статистики (Росстат)

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

1. МойОфис;
2. Astra Linux Special Edition;

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

1. Электронный периодический справочник "Система ГАРАНТ";
2. КонсультантПлюс;

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СИ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СИ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СИ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СИ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения