Федеральное государственное автономное образовательное учреждение высшего образования
"Самарский государственный экономический университет"

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

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: 3 з.е.
в академических часах: 108 ак.ч.

г. Самара, 2026

Разработчики:
Кандидат наук Ткаченко С. П.

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:

- Принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий действий;
- Выявлять, документировать, пресекать и раскрывать преступления и иные правонарушения в сфере экономики.

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

Компетенции, индикаторы и результаты обучения

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

УК-1.2 Принимает конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий действий

Знать:

УК-1.2/Зн1 Решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий действий

Уметь:

УК-1.2/Ум1 Осуществлять критический анализ проблемных ситуаций на основе системного подхода

Владеть:

УК-1.2/Нв1 Навыками создания эффективных процедур анализа проблем, принятия решений и разработки стратегий действий

ПК-4 Способен планировать и организовывать служебную деятельность подчиненных, правил внутреннего контроля в целях ПОД/ФТ

ПК-4.1 Выявляет, документирует, пресекает и раскрывает преступления и иные правонарушения в сфере экономики

Знать:

ПК-4.1/Зн1 Процедуры по документированию, пресечению и раскрытию преступлений и иных правонарушений в сфере экономики

Уметь:

ПК-4.1/Ум1 Планировать и организовывать служебную деятельность подчиненных, правил внутреннего контроля в целях ПОД/ФТ

Владеть:

ПК-4.1/Нв1 Методиками выявления, документирования и раскрываемости преступлений и иных правонарушений в сфере экономики

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Информационная безопасность» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): Очная форма обучения - 10, Очно-заочная форма обучения - 10.

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

Компетенция	Предшествующие дисциплины	Последующие дисциплины
ПК-4 - Способен планировать и организовывать служебную деятельность подчиненных, правил внутреннего контроля в целях ПОД/ФТ		
ПК-4.1 Выявляет, документирует, пресекает и раскрывает преступления и иные правонарушения в сфере экономики	Нефинансовая отчетность экономических субъектов, Организация и методика проведения налоговых проверок, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика, Финансовая безопасность	Нефинансовая отчетность экономических субъектов, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Производственная практика: преддипломная практика
УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий		
УК-1.2 Принимает конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий действий	История государства и права зарубежных стран, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Учебная практика: ознакомительная практика, Философия, Экономическая теория	Подготовка к процедуре защиты и защита выпускной квалификационной работы

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
Десятый семестр	108	3	36	18	18	0,15	53,85	Зачет
Всего	108	3	36	18	18	0,15	53,85	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
Десятый семестр	108	3	4	2	2	0,15	85,85	Зачет
Всего	108	3	4	2	2	0,15	85,85	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. Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем в КФС	**44**	**9**	**9**	**26**
Тема 1.1. Понятие защиты информационной системы. Цель защиты информации. Нормативно-правовая база функционирования систем защиты информации. Угрозы безопасности автоматизированным системам КФС и их классификация.	44	9	9	26
Раздел 2. Способы защиты автоматизированных систем КФС от угроз информационной безопасности	**45,85**	**9**	**9**	**27,85**

Тема 2.1. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа. Частная модель нарушителя. Определение, классификация и общая характеристика технических каналов утечки информации. Понятие контролируемой зоны и методы определения ее размеров.	45,85	9	9	27,85

Очно-заочная форма обучения

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа
Раздел 1. Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем в КФС	**44**	**1**	**1**	**42**
Тема 1.1. Понятие защиты информационной системы. Цель защиты информации. Нормативно-правовая база функционирования систем защиты информации. Угрозы безопасности автоматизированным системам КФС и их классификация.	44	1	1	42
Раздел 2. Способы защиты автоматизированных систем КФС от угроз информационной безопасности	**45,85**	**1**	**1**	**43,85**

Тема 2.1. Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа. Частная модель нарушителя. Определение, классификация и общая характеристика технических каналов утечки информации. Понятие контролируемой зоны и методы определения ее размеров.	45,85	1	1	43,85

5.2. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	тестирование
Промежуточная аттестация	Зачет

№ п/п	Наименование раздела	Вид контроля/ используемые оценочные материалы	
		Текущий	Промежут. аттестация
1	Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем в КФС	тестирование	Зачет
2	Способы защиты автоматизированных систем КФС от угроз информационной безопасности	тестирование	Зачет

6. Оценочные материалы текущего контроля

1. Стандарты и нормативные документы, регламентирующие понятия и классификацию угроз и уязвимостей автоматизированных систем в КФС тестирование

№ п/п	Содержание вопроса		Компетенция
	Правильный ответ (ключ ответа)		
1	Выберите один правильный ответ Кто является основным ответственным за определение уровня классификации информации? 1. Руководитель среднего звена 2. Высшее руководство 3. Владелец 4. Пользователь		УК-1
	Ответ:	3. Владелец	
2	Выберите один правильный ответ Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? 1. Сотрудники 2. Хакеры 3. Атакующие 4. Контрагенты (лица, работающие по договору)		УК-1
	Ответ:	1. Сотрудники	

3	Выберите один правильный ответ Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? 1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования 2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации 3. Улучшить контроль за безопасностью этой информации 4. Снизить уровень классификации этой информации Ответ: 3. Улучшить контроль за безопасностью этой информации	УК-1
4	Выберите один правильный ответ Что самое главное должно продумать руководство при классификации данных? 1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным 2. Необходимый уровень доступности, целостности и конфиденциальности 3. Оценить уровень риска и отменить контрмеры 4. Управление доступом, которое должно защищать данные Ответ: 2. Необходимый уровень доступности, целостности и конфиденциальности	УК-1
5	Выберите один правильный ответ Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? 1. Владельцы данных 2. Пользователи 3. Администраторы 4. Руководство Ответ: 4. Руководство	УК-1
6	Выберите один правильный ответ Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? 1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски 2. Когда риски не могут быть приняты во внимание по политическим соображениям 3. Когда необходимые защитные меры слишком сложны 4. Когда стоимость контрмер превышает ценность актива и потенциальные потери Ответ: 4. Когда стоимость контрмер превышает ценность актива и потенциальные потери	УК-1
7	Выберите один правильный ответ Что такое политики безопасности? 1. Пошаговые инструкции по выполнению задач безопасности 2. Общие руководящие требования по достижению определенного уровня безопасности 3. Широкие, высокоуровневые заявления руководства 4. Детализированные документы по обработке инцидентов безопасности Ответ: 2. Общие руководящие требования по достижению определенного уровня безопасности	УК-1
8	Выберите один правильный ответ Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности? 1. Поддержка 2. Выполнение анализа рисков 3. Определение цели и границ 4. Делегирование полномочий Ответ: 2. Выполнение анализа рисков	УК-1
9	Задание закрытого типа на установление правильной последовательности Реализуя свою профессиональную деятельность укажите характерные черты пользователей информации ограниченного доступа 1. Ответственным за определение уровня классификации информации? А. Сотрудник 2. Какая фигура категория является наиболее рискованной для компании Б. Руководитель 3. Кто несет ответственность за то, что данные классифицированы и защищены? В. Владелец Ответ: 1 - В 2 - А 3 - Б	УК-1
10	Укажите возможные ответы Осуществляя свою профессиональную деятельность администратор случайно обнаруживает в логах сервера странные записи, указывающие на попытку SQL-инъекции в форме авторизации корпоративного портала. Каковы ваши первые шаги в течение следующих 30 минут Ответ: Остановить атаку — заблокировать IP- адрес злоумышленника на межсетевом экране	УК-1

11	Дайте единственно верный вариант ответа Осуществляя профессиональную деятельность в качестве администратора сети необходимо новому сотруднику дать доступ к корпоративным ресурсам		УК-1
	Ответ:	Получить официальную заявку от начальника функционального отдела куда устраивается сотрудник: 1. Должность и конкретные обязанности. 2. Точный список необходимых систем, программ и прав доступа. 3. В службе каталогов создать учетную запись пользователя по утвержденному шаблону	
12	Дайте единственно верный вариант ответа Под угрозой безопасности информации при создании информационной системы понимается		УК-1
	Ответ:	Потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба информации	
13	Дайте единственно верный вариант ответа Современные информационные технологии к внутренним нарушителям информационной безопасности относят		УК-1
	Ответ:	Сотрудников организации	
14	Дайте единственно верный вариант ответа Современные информационные технологии определяют ЭЦП как: 1. электронно-цифровой преобразователь 2. электронно-цифровая подпись 3. электронно-цифровой процессор		УК-1
	Ответ:	2. электронно-цифровая подпись	
15	Выберите один правильный ответ К аспектам информационной безопасности не относится: 1. Доступность 2. Целостность 3. Конфиденциальность 4. Защищенность		УК-1
	Ответ:	4. Защищенность	

2. Способы защиты автоматизированных систем КФС от угроз информационной безопасности тестирование

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	Укажите один правильный ответ Кодирование информации - это 1. представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д. 2. метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом		ПК-4
	Ответ:	1. представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.	
2	Укажите один правильный ответ Наука о скрытой передаче информации путем сохранения в тайне самого факта передачи - это 1) Стеганография 2) Криптография 3) Криптоанализ		ПК-4
	Ответ:	1) Стеганография	
3	Укажите один правильный ответ Под непреднамеренным воздействием на защищаемую информацию понимают? 1. Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений 2. Процесс ее преобразования, при котором содержание информации изменяется на ложную 3. Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию 4. Не ограничения доступа в отдельные отрасли экономики или на конкретные производства		ПК-4
	Ответ:	1. Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений	
4	Укажите один правильный ответ Основные предметные направления Защиты Информации? 1. Охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности 2. Охрана золотого фонда страны 3.Определение ценности информации 4. Совершенствование скорости передачи информации		ПК-4
	Ответ:	1. Охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности	

5	Укажите один правильный ответ Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право 1. управление доступом 2. конфиденциальность 3. аутентичность 4. целостность 5. доступность Ответ: 2. конфиденциальность	ПК-4
6	Укажите один правильный ответ Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем 1. защита от сбоев в электропитании 2 защита от сбоев серверов, рабочих станций и локальных компьютеров 3. защита от сбоев устройств для хранения информации 4. защита от утечек информации электромагнитных излучений Ответ: 2. защита от сбоев серверов, рабочих станций и локальных компьютеров	ПК-4
7	Укажите один правильный ответ Какая из перечисленных атак на поток информации является пассивной: 1. перехват. 2. имитация. 3. модификация. 4. фальсификация. 5. прерывание. Ответ: 1. перехват.	ПК-4
8	Укажите один правильный ответ К открытым источникам информация относятся. 1. Газеты, Радио, Новости 2. Информация украденная у спецслужб 3. Из вскрытого сейфа 4. Украденная из правительственной организации Ответ: 1. Газеты, Радио, Новости	ПК-4
9	Укажите один правильный ответ Технические каналы утечки информации делятся на… 1. Акустические и виброакустические 2.Электрические 3. Оптические 4. Все перечисленное Ответ: 4. Все перечисленное	ПК-4
10	Укажите один правильный ответ Какие выделить направления мер информационной безопасности 1. Правовые 2. Организационные 3. Все ответы верны 4. Технические Ответ: Все ответы верны	ПК-4
11	Дайте допустимый ответ Решая задачи администрирования сети обнаруживаете, что политика паролей в компании устарела и имеет следующие требования: 1. Минимальная длина пароля: 6 символов. 2. Обязательный набор символов: не регламентирован (можно использовать только цифры). Ваши действия Ответ: Увеличить длину пароля: минимальная длина должна быть увеличена до не менее 12 символов с использованием символов верхнего, нижнего регистров и цифр	ПК-4
12	Дайте допустимый ответ СКУД блокирует доступ при предъявлении пропуска штатному сотруднику организации в серверную комнату для осуществления им своей профессиональной деятельности Ответ: Не пропускать сотрудника, зафиксировать попытку доступа, сообщить руководству	ПК-4
13	Дайте допустимый ответ Сотрудником при решении поставленной задачи в начале рабочего дня регистрируется жалоба 1. Необъяснимо медленную работу компьютеров. 2. Появление всплывающих окон с рекламой (в том числе на русском языке, предлагающие установить какие-то "утилиты для очистки"). 3. Самопроизвольное изменение домашней страницы в браузере на неизвестный поисковый портал. Ответ: Администратору компьютерной сети немедленно отключить пораженный компьютер от локальной сети. Проверить журналы антивируса.	ПК-4

14	Дайте допустимый ответ Во время осуществления своей профессиональной деятельности сотрудник обратился в отдел ИБ в связи с тем, что часть файлов оказалась зашифрована.		ПК-4
	Ответ:	Администратору сети изолировать рабочее место от сети. Оповестить руководителя. Сохранить доказательства. Восстановить данные из резервной копии.	
15	Дайте допустимый ответ Используя информационные технологии получаете электронное письмо от якобы службы поддержки популярного облачного сервиса, которым вы пользуетесь. Письмо выглядит срочным: «Ваша учетная запись будет заблокирована в течение 24 часов!». В письме есть кнопка «Восстановить доступ»		ПК-4
	Ответ:	Нельзя нажимать на ссылку и открывать вложения, если они есть. Внимательно изучить адрес отправителя. Немедленно переслать это письмо в IT-отдел или службу информационной безопасности.	

7. Оценочные материалы промежуточной аттестации

Зачет десятый семестр - очная, очно-заочная

№ п/п	Содержание вопроса		Компетенция
		Правильный ответ (ключ ответа)	
1	Дайте развернутый ответ на вопрос Информационные технологии требуют идентификация и аутентификация пользователей		УК-1, ПК-4
	Ответ:	Идентификация — это процесс, когда информационная система определяет, существует конкретный пользователь или нет, с помощью идентификатора. Аутентификация — это процесс, когда пользователь вводит ключ, например пароль или пин-код, подтверждая своё право на доступ к учётной записи и хранящейся в ней информации. При входе в соцсеть у пользователя могут попросить не только пароль, но и другую информацию — код из СМС или биометрические данные.	
2	Дайте развернутый ответ на вопрос При работе с информационными технологиями сталкиваются с несанкционированным доступом		ПК-4, УК-1
	Ответ:	Несанкционированный доступ это получение данных без разрешения владельца, нарушающее право на конфиденциальность. Основные способы: Технические: Атаки на уязвимости. Фишинг — способ обмана пользователей для получения их личных данных Перехват трафика. Организационные: Возможен физический доступ. Социальная инженерия: Злоумышленник манипулирует сотрудниками. Внутренний доступ: От сотрудников с разрешённым доступом, которые используют свои полномочия неправомерно.	
3	Дайте развернутый ответ на вопрос При использовании информационных технологий необходима физическая защита компьютеров		УК-1, ПК-4
	Ответ:	Включает в себя конструкции и устройства, которые препятствуют проникновению нежелательных лиц в помещения и ограничивают доступ к рабочим местам сотрудников. Включает: Контроль через учётные записи пользователей. Аппаратные системы защиты и контроля доступа. Криптографическое закрытие защищаемой информации, хранимой на носителях и архивация данных.	
4	Дайте развернутый ответ на вопрос. Осуществляя профессиональную деятельность необходимо классифицировать компьютерные вирусы.		УК-1, ПК-4
	Ответ:	Вирус - это программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению. В зараженной программе исходный код изменяется таким образом, чтобы вирус получил управление первым, до начала работы программы- вирусоносителя. При передаче управления вирусу он каким-либо способом находит новую программу и выполняет вставку собственной копии в начало или добавление ее в конец этой, обычно еще не зараженной, программы.	
5	Дайте развернутый ответ на вопрос. Лицензирование и в области защиты персональных данных при реализации информационных технологий		ПК-4, УК-1
	Ответ:	Основные понятия в области лицензирования и сертификации даны Федеральными законами «О лицензировании отдельных видов деятельности» от 8 августа 2001 г. № 128-ФЗ . Лицензия – специальное разрешение на осуществление конкретного вида деятельности выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю. Лицензирование – мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий	
6	Дайте развернутый ответ на вопрос. Российская Федерация используя информационные технологии подвергается угрозам		УК-1, ПК-4
	Ответ:	Под угрозой информационной безопасности понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности или секретности информации. Угрозы конституционным правам и свободам человека и гражданина. Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации. Угрозы безопасности информационных и телекоммуникационных средств и систем как уже развернутых, так и создаваемых на территории России.	

7	Дайте развернутый ответ на вопрос Для решения профессиональной задачи необходимо определить требования к построению систем безопасности предприятия		ПК-4, УК-1
	Ответ:	Предотвращение ущерба деятельности за счет разглашения, утечки и несанкционированного доступа к источникам конфиденциальной информации; пресечение хищения финансовых и материально-технических средств, уничтожения имущества и ценностей. Нарушения работы технических средств обеспечения производственной деятельности, включая средства информатизации. Предотвращение ущерба персоналу предприятия. Обеспечение безопасности не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов.	
8	Дайте развернутый ответ на вопрос Современные информационные технологии подвергаются угрозам информационной безопасности		УК-1, ПК-4
	Ответ:	Угрозы зависят от интересов субъектов информационных отношений (какой ущерб является для них неприемлемым). Реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. К основным угрозам безопасности относят: • раскрытие конфиденциальной информации; • компрометация информации; • несанкционированное использование информационных ресурсов; • ошибочное использование ресурсов	
9	Дайте развернутый ответ на вопрос Для решения поставленной задачи по защите данных какие использовать методы обеспечения информационной безопасности Российской Федерации		УК-1, ПК-4
	Ответ:	Предотвращение ущерба деятельности за счет разглашения, утечки и несанкционированного доступа к источникам конфиденциальной информации; пресечение хищения финансовых и материально-технических средств, уничтожения имущества и ценностей. Нарушения работы технических средств обеспечения производственной деятельности, включая средства информатизации. Предотвращение ущерба персоналу предприятия. Обеспечение безопасности не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов. Угрозы зависят от интересов субъектов информационных отношений (какой ущерб является для них неприемлемым). Реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. К основным угрозам безопасности относят: • раскрытие конфиденциальной информации; • компрометация информации; • несанкционированное использование информационных ресурсов; • ошибочное использование ресурсов Правовые методы обеспечения информационной безопасности Российской Федерации: нормативно правовые акты и нормативно методические документы по вопросам обеспечения информационной безопасности Российской Федерации. Организационно-техническимие методы обеспечения информационной безопасности Российской Федерации: создание и совершенствование системы обеспечения информационной безопасности Российской Федерации; усиление правоприменительной деятельности федеральных органов исполнительной власти; создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации	
10	Дайте развернутый ответ на вопрос Профессиональные организации составляющие силы обеспечения информационной безопасности Российской Федерации		УК-1, ПК-4
	Ответ:	Основу сил обеспечения информационной безопасности РФ составляют органы исполнительной власти. Для этого эти органы имеют соответствующие части, подразделения и службы. К ним относятся: 1. Федеральная служба безопасности Российской Федерации (ФСБ); 2. Служба внешней разведки Российской Федерации (СВР); 3. Федеральная служба по техническому и экспортному контролю 4. (ФСТЭК – бывшая Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России); 5. Министерство внутренних дел Российской Федерации (МВД); 6. Органы судебной власти Российской Федерации; 7. Федеральная таможенная служба Российской Федерации; 8. Федеральная служба по техническому регулированию и метрологии Российской Федерации.	
11	Дайте развернутый ответ на вопрос Профессиональная деятельность ФСТЭК при сертификации СЗИ		УК-1, ПК-4

	Ответ:	1. создает систему сертификации средств защиты информации по требованиям безопасности информации 2. аккредитует органы по сертификации средств защиты информации и испытательные лаборатории; 3. осуществляет выбор способа подтверждения соответствия средств защиты информации требованиям нормативных документов; 4. устанавливает правила аккредитации органов по сертификации средств защиты информации и испытательных лабораторий; 5. выдает сертификаты и лицензии на применение знака соответствия; 6. ведет государственный реестр участников сертификации и сертифицированных средств защиты информации	

7.1. Уровни овладения

Компетенция: УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Индикатор достижения компетенции: УК-1.2 Принимает конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий действий.

Уровень	Характеристика	Оценка в баллах
Повышенный	Способен осуществлять глубокий анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий Принимает верные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий действий	81-100
Базовый	Способен осуществлятьобщий анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий Принимает в осноснос правильные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий действий	61-80
Пороговый	Способен осуществлять поверхностный анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий Принимаетчастично правилтные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий действий	41-60
Ниже порогового	Компетенция не освоена	0-40

Компетенция: ПК-4 Способен планировать и организовывать служебную деятельность подчиненных, правил внутреннего контроля в целях ПОД/ФТ.

Индикатор достижения компетенции: ПК-4.1 Выявляет, документирует, пресекает и раскрывает преступления и иные правонарушения в сфере экономики.

Уровень	Характеристика	Оценка в баллах
Повышенный	В полном объме выявляет, документирует, пресекает и раскрывает преступления и иные правонарушения в сфере экономики	81-100
Базовый	С незначительными оибками выявляет, документирует, пресекает и раскрывает преступления и иные правонарушения в сфере экономики	61-80

Пороговый	Не вполном объеме выявляет, документирует, пресекает и раскрывает преступления и иные правонарушения в сфере экономики	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. 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. Меркулова, Е. Ю. Общая экономическая безопасность: учебник и практикум для вузов / Е. Ю. Меркулова. - 2-е изд. - Москва: Юрайт, 2026. - 528 с - 978-5-534-16403-9. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588408 (дата обращения: 21.05.2026). - Режим доступа: по подписке

Дополнительная литература

1. Суворова, Г. М. Информационная безопасность: учебник для вузов / Г. М. Суворова. - 2-е изд. - Москва: Юрайт, 2026. - 277 с - 978-5-534-16450-3. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/588515 (дата обращения: 21.05.2026). - Режим доступа: по подписке

2. Щербак, А. В. Информационная безопасность: учебник для вузов / А. В. Щербак. - 2-е изд. - Москва: Юрайт, 2026. - 252 с - 978-5-9916-4299-6. - Текст: электронный // ИКО Юрайт: [сайт]. - URL: https://urait.ru/bcode/589902 (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

Не используются.

Ресурсы «Интернет»

1. https://digital.gov.ru - Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России)
2. http://www.gov.ru/) - http://www.gov.ru/)
3. https://lms2.sseu.ru - БРСО

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. LibreOffice;
2. 7-Zip;
3. «Альт Образование» и/или «Альт Рабочая станция»;

Перечень информационно-справочных систем
(обновление выполняется еженедельно)

Не используется.

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 СГ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения