МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

03.12.2025 г.

протокол № 6

Зав. кафедрой Антипин И.А.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025 г.

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Корпоративная безопасность
Специальность	38.05.01 Экономическая безопасность
Специализация	Экономическая безопасность
Форма обучения	очная
Год набора	2026

Разработана:
Доцент, к.э.н.
Ефимова Е.Г.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональнойобразовательной программы высшего образования - программы специалитета, разработанной всоответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования-специалитет по специальности 38.05.01 Экономическая безопасность (приказМинобрнауки России от 14.04.2021 г. № 293)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

формирование компетенций, направленных на получение прочных знаний методологическихи методических основ и принципов обеспечения корпоративной безопасности, ознакомление ссистемой методов, применяемых в обеспечении корпоративной безопасности, выработки уменийпринятия научно-обоснованных решений в обеспечении экономической безопасностихозяйствующих субъектов, формирование способности оценки полученных результатов дляразработки рекомендаций по укреплению корпоративной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточнаяаттестация	Часов					З.е.
	Всего засеместр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числеподготовкаконтрольных икурсовых	
		Всего	Лекции	Практическиезанятия, включаякурсовоепроектирование		
Семестр 8						
Зачет с оценкой	108	64	32	32	44	3

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции,установленные в соответствии ФГОС ВО.

Шифр и наименованиекомпетенции	Индикаторы достижения компетенций
организационно-управленческий	

ПК-3 Планирование,внедрение и реализациярискориентированногоподхода к управлениюорганизацией, в т.ч.кредитной организацией,целеполагания и программмотивации с учетом рисков,постановка целей длявнедрения риск-менеджмента	ИД-1.ПК-3 Знать: Законодательство Российской Федерации по виду деятельностиорганизации и требования (рекомендации) области управлениярисками; Международные и российские стандарты по риск-менеджменту и риск-ориентированному управлению организацией; Корпоративные финансы, теория вероятности и математическаястатистика, корпоративное управление, поведенческая экономика,нейроэкономика и теория принятия решений; Перечень заинтересованных сторон; Организацию управленческой отчетности организации, отдельныхбизнес-процессов, проек-тов, решений; Цели организации, цели и задачи бизнес-процессов, цели ключевыхуправленческих реше-ний; Организационную структуру организации; Органы управления организации; Подходы к управлению, методы и инструменты управления рисками, втом числе оценки рисков, включая идентификацию и анализ влиянийрисков на цели организации и ключевые показатели деятельности,приоритизации рисков, определения критериев существенности; Состав, форму и порядок формирования отчетности с учетом рисков; Модели зрелости в области управления рисками; Подходы к реализации и методы реализации риск-ориентированногоуправления организаци-ей; Методы формирования дорожной карты внедрения риск-ориентированного подхода к управ-лению организацией; Программное обеспечение в области риск-ориентированногоуправления организацией, оценки влияния рисков на целиорганизации; Подходы к коммуникации и доведению информации доисполнительных органов и совета директоров; Нормы профессиональной этики; Профессиональные сообщества; Иностранный язык в объеме, необходимом для выполнения трудовойфункции;

ПК-3 Планирование,внедрение и реализациярискориентированногоподхода к управлениюорганизацией, в т.ч.кредитной организацией,целеполагания и программмотивации с учетом рисков,постановка целей длявнедрения риск-менеджмента	ИД-2.ПК-3 Уметь: Определять заинтересованные стороны в реализации риск-ориентированного управления в организации на уровне акционеров,совета директоров, партнеров, руководства организации; Выстраивать коммуникации с заинтересованными сторонами; Формировать концепции реализации риск-ориентированного подхода ворганизации; Формировать и представлять отчеты о внедрении риск-ориентированного подхода к управле-нию организациейзаинтересованным сторонам; Представлять и согласовывать внутренние методологические иорганизационно-распорядительные документы по управлению рисками(политика, принципы, цели, задачи); Принимать решения о выборе программного обеспечения дляреализации риск-ориентированного управления организацией иосуществлять координацию работы по внед-рению; Развивать культуру риск-ориентированного управления организацией ипроводить обучение для заинтересованных сторон; Формировать и представлять материалы о достижениях организации вобласти управления рисками в рамках профессиональных сообществ; Изучать лучшую практику внедрения риск-ориентированногоуправления на предмет приме-нения в организации; Создавать и воспроизводить видеоролики, презентации, слайд-шоу,медиафайлы и итоговую продукцию из исходных аудиокомпонентов,визуальных и мультимедийных компонентов;

ПК-3 Планирование,внедрение и реализациярискориентированногоподхода к управлениюорганизацией, в т.ч.кредитной организацией,целеполагания и программмотивации с учетом рисков,постановка целей длявнедрения риск-менеджмента	ИД-3.ПК-3 Иметь практический опыт: Определения заинтересованных сторон на уровне акционеров, советадиректоров, партнеров, руководства организации; Создания каналов коммуникации с заинтересованными сторонами дляформирования кон-цепции и реализации риск-ориентированногоподхода и представления отчетов о внедрении; Формирования и согласования концепции развития риск-ориентированного подхода к управ-лению организацией, ключевыхцелей, задач и шагов внедрения риск-ориентированного управления,включая встраивание рисков в существующие инструментыпланирования: фи-нансовые модели, планы-графики реализациипроектов, инструменты, связанные с бизнес-процессами илипринимаемыми решениями, инструменты формирования имониторинга реа-лизации мотивационной программы; Согласования внутренних методологических и организационно-распорядительных докумен-тов по управлению рисками (политика,принципы, цели, задачи); Предоставления и согласования с заинтересованными сторонамидорожной карты внедрения риск-ориентированного подхода куправлению организацией с определением необходимых ресурсов,ролей и ответственности, а также отчетов о ее реализации; Выбора программного обеспечения для реализации риск-ориентированного управления орга-низацией и координации работы повнедрению; Развития культуры и обучение акционеров, совета директоров,партнеров, руководства орга-низации в области риск-ориентированного управления организацией;
расчетно-экономический	

ПК-2 Работа в процессепринятия решений,связанных снеопределенностью ворганизации, в т.ч.кредитной организации	ИД-1.ПК-2 Знать: Законодательство Российской Федерации по виду деятельностиорганизации и требования (рекомендации) области управлениярисками; Корпоративные финансы, теория вероятности и математическаястатистика, корпоративное управление, поведенческая экономика,нейроэкономика и теория принятия решений; Перечень заинтересованных сторон; Органы управления организации и порядок их работы; Подходы к управлению, методы и инструменты управления рисками, втом числе оценки рисков, включая идентификацию и анализ влияниярисков на цели организации и ключевые показатели деятельности,приоритизации рисков, определения критериев существенности; Критерии для принятия управленческих решений; Форматы и подходы к подготовке информации о влиянии рисков нацели организации, цели бизнес-процессов, цели управленческихрешений, а также к обеспечению исполнения требо-ваний регуляторови доведения такой информации до органов принятия решений; Виды и способы коммуникации с представителями руководстваорганизации и бизнес-процессов при подготовке материалов дляуправленческих решений; Нормы профессиональной этики; Нормы профессиональной этики; Иностранный язык в объеме, необходимом для выполнения трудовойфункции; Основы осуществления защиты персональных данных; Основы работы в операционных системах; Принципы соблюдения информационной безопасности, сохраненияконфиденциальности данных.

ПК-2 Работа в процессепринятия решений,связанных снеопределенностью ворганизации, в т.ч.кредитной организации	ИД-2.ПК-2 Уметь: Формировать, представлять и согласовывать критерии принятияуправленческих решений с учетом результатов оценки влияния рисковна цели организации (выполнение требований регуляторов изаинтересованных сторон); Выстраивать коммуникации с заинтересованными сторонами; Представлять результаты применения инструментов риск-менеджментапри оценке рисков, включая идентификацию и анализ влияния рисковна цели организации (выполнение требо-ваний регуляторов изаинтересованных сторон); Согласовывать результаты применения инструментов риск-менеджмента при оценке рисков, включая идентификацию и анализвлияния рисков на цели организации (выполнение требо-ванийрегуляторов и заинтересованных сторон); Организовывать работу по подготовке и раскрытию в рамкахстратегических решений, бюд-жетирования, управления ключевымипроектами информации о результатах оценки рисков и их влиянии нацели организации (выполнение требований регуляторов изаинтересованных сторон); Создавать и воспроизводить видеоролики, презентации, слайд-шоу,медиафайлы и итоговую продукцию из исходных аудиокомпонентов,визуальных и мультимедийных компонентов; Применять подходы безопасной работы в информационно-телекоммуникационной сети "Ин-тернет" (защита персональныхданных, антивирусная защита, информационная гигиена); Управлять размещением цифровой информации, в том числе вдисковых хранилищах локаль-ной и глобальной компьютерной сети; Формировать медиатеки для структурированного хранения икаталогизации цифровой ин-формации.
	ИД-3.ПК-2 Иметь практический опыт: Формирования (актуализации) критериев принятия управленческихрешений с учетом ре-зультатов оценки влияния рисков на целиорганизации (выполнение требований регуляторов и заинтересованныхсторон); Выстраивания коммуникации и согласования результатов применениянструментов риск-менеджмента при оценке рисков, включаяидентификацию и анализ влияния рисков на цели организации(выполнение требований регуляторов и заинтересованных сторон); Организации подготовки и раскрытия в рамках стратегическихрешений, бюджетирования, управления ключевыми проектамиинформации о результатах оценки рисков и их влиянии на целиорганизации (выполнение требований регуляторов и заинтересованныхсторон).

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост.работа	Контрольсамостоятельной работы
			Лекции	Лабораторные	Практическиезанятия		
Семестр 8		108					

Тема 1.	Корпоративная безопасность: понятие,сущность, структурные элементы (ПК-2,ПК-3)	16	4		4	8	
Тема 2.	Основы обеспечения информационнойбезопасности (ПК-2,	16	6		4	6	
Тема 3.	Кадровая безопасность (ПК-2, ПК-3)	16	6		4	6	
Тема 4.	Экономическая безопасностькорпорации. Экономическаяпаразитология (ПК-2, ПК-3)	18	6		6	6	
Тема 5.	Основы инженерно-техническойбезопасности (ПК-2, ПК-3)	13	3		4	6	
Тема 6.	Бизнес-разведка (ПК-2, ПК-3)	16	4		6	6	
Тема 7.	Организационные основы обеспечениякорпоративной безопасности (ПК-2, ПК-3)	13	3		4	6	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочногосредства	Описание оценочного средства	Критериоценивания
Текущий контроль (Приложение 4)			
темам 1, 2, 3,4, 5, 6, 7	вопросы по темам	Вопросы для собеседования на семинаре. Оценивается полнота и достоверностьизложения материала, использованиедополнительных источников информации поданной теме, умение грамотно, четко,структурировано излагать свои мысли,выслушать товарищей, сделать выводы повопросу.	от 0 до 5 баллов завопросы покаждой теме
темы 2; 3; 5	тест	Тест из 15 вопросов закрытого типа повариантам.	от 0 до 5 баллов затест по одной теме
темы 3; 4; 5;6	индивидуальноезадание	Комплект индивидуальных заданий длявыполнения расчётов, оценке и развёрнутогоанализа состояния безопасностиисследуемого объекта (по темам курса).Предлагаются конкретные задачи назакрепление материала, практическоеприменение полученных по дисциплинезнаний. Оценивается правильность,аргументированность решения задачи,структурированность и	по 5 баллов закаждое задание
тема 7	тест	Итоговый тест из 30 вопросов, обобщающийвсе пройденные темы курса (смешанноготипа). Примерные вопросы итогового тестапредставлены в тестах по	от 0 до 5 баллов
Промежуточная аттестация (Приложение 5)			
8 семестр(ЗаО)	билет для зачёта соценкой	Билет включает 1 теоретический вопрос и 1практическое задание	100 баллов (по 50баллов за каждыйвопрос билета)

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущего контроляи промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показываетуровень подготовки студента.

Текущий контроль. Используется 100-балльная система оценивания. Оценка работы студентав течении семестра осуществляется преподавателем в соответствии с разработанной им системойоценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущей аттестации,планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, поооценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, тоданный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работыстудента по окончанию дисциплины (части дисциплины) осуществляется преподавателем всоответствии с разработанной им системой оценки достижений студента в процессе обучения поданной дисциплине. Промежуточная аттестация также проводится по окончанию формированиякомпетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, впятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме,понимают, самостоятельно умеют применять,исследовать, идентифицировать, анализировать,систематизировать, распределять по категориям,рассчитать показатели, классифицировать,разрабатывать модели, алгоритмизировать, управлять,организовать, планировать процессы исследования,осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме,понимают, самостоятельно умеют применять,исследовать, идентифицировать, анализировать,систематизировать, распределять по категориям,рассчитать показатели, классифицировать,разрабатывать модели, алгоритмизировать, управлять,организовать, планировать процессы исследования,осуществлять оценку результатов. Могут быть допущены недочеты, исправленныестудентом самостоятельно в процессе работы (ответаи т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеютприменять, исследовать, идентифицировать,анализировать, систематизировать, распределять покатегориям, рассчитать показатели,классифицировать, разрабатывать модели,алгоритмизировать, управлять, организовать,планировать процессы исследования, осуществлятьоценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняетсяисправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическимизнаниями, не умеют самостоятельно применять,исследовать, идентифицировать, анализировать,систематизировать, распределять по категориям,рассчитать показатели, классифицировать,разрабатывать модели, алгоритмизировать, управлять,организовать, планировать процессы исследования,осуществлять оценку результатов. Не сформированы умения и навыки для
100% - 50%	зачтено	характеристика показателя соответствует «отлично»,«хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует«неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Корпоративная безопасность: понятие, сущность, структурные элементы (ПК-2, ПК-3)
Корпоративная безопасность: определение, цель, задачи, составные элементы. Объекты и субъектыобеспечения корпоративной безопасности. Варианты (уровни) субъектов обеспечениякорпоративной безопасности. Основные виды угроз корпоративной безопасности. Характеристикаэлементов системы корпоративной безопасности. Принципы построения корпоративнойбезопасности.

Тема 2. Основы обеспечения информационной безопасности (ПК-2, ПК-3)
Информационная безопасность. Правовые основы информационной безопасности компании.Коммерческая тайна компании. Информационная безопасность и правоохранительные органы взаконодательстве РФ. Построение системы информационной безопасности компании.Международные стандарты по информационной безопасности и концепции системного подхода кзащите информации. IT – безопасность. Угрозы электронным информационным ресурсам. Типовыесценарии НСД к электронным информационным ресурсам и защита от них. Криптографическаязащита информации. Электронная цифровая подпись. Защита от утери электронныхинформационных ресурсов. Антивирусная защита информационных ресурсов. Защита информациив автономных информационных системах. Защита информационных сетей компании. Защитаинформационных ресурсов от хакерских атак из Интернета. Защита информации с использованиемсистем Honeypot. Защита информации от продуктов-шпионов. Анализ особенностей российскогорынка IT- безопасности

Тема 3. Кадровая безопасность (ПК-2, ПК-3)
Оперативная работа с кадрами. Организация кадровой работы в компании. Мотивация персоналакомпании. Лояльность сотрудников компании. Прием-увольнение сотрудников. Применениеполиграфа в тестировании сотрудников компании. Порядок приобретения, хранения, ношения ипримененияоружия. Психология безопасного поведения. Основы невербального общения с людьми.Различные способы получения конфиденциальной информации у сотрудников компании.

Тема 4. Экономическая безопасность корпорации. Экономическая паразитология (ПК-2, ПК-3)
Понятие «экономическая безопасность организации», «экономическая безопасность корпорации».Структура экономической безопасности корпорации. Система и методы анализа и управленияэкономическими рисками. Виды экономических рисков. Методы оценки экономических рисков.Методы управления экономическими рисками.
Мошенничество: понятие, виды. Внутреннее и внешнее мошенничество. Признаки мошенничества.Выявление мошенничества. Основные способы устранения возможностей мошенничества.
Враждебное (недружественное) поглощение: понятие, виды, схемы. Основные цели враждебногопоглощения. Возможные варианты враждебного поглощения. Некоторые способы предотвращениявраждебного поглощения. Возможные способы защиты от начавшегося враждебного поглощения.Компании-агрессоры. Гринмейл.

Тема 5. Основы инженерно-технической безопасности (ПК-2, ПК-3)
Охранные мероприятия. Противопожарная безопасность. Системы охраны периметров. Охранноетелевидение. Системы охранных сигнализаций. Контрольно-пропускной режим в компании.Биометрические системы распознавания личности.

Тема 6. Бизнес-разведка (ПК-2, ПК-3)
Бизнес-разведка: понятие, задачи, направления проведения. Понятие «информационное задание» вбизнес-разведке. Методы сбора информации, применяемые в бизнес-разведке. Способыофициального получения информации из государственных органов. Сбор информации в сетиИнтернет. Аналитические методы бизнес-разведки.

Тема 7. Организационные основы обеспечения корпоративной безопасности (ПК-2, ПК-3)
Варианты организации обеспечения безопасности компании. Аутсорсинг безопасности. Цели изадачи обеспечения безопасности компании. Принципы организации и функционирования системыбезопасности компании. Средства обеспечения безопасности.
Служба безопасности компании: понятие, структура. Методы проверки работы службыбезопасности. Внутри объектовый режим. Пропускной режим. Система мер защиты компании.Управление системой безопасности компании.

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Основы обеспечения информационной безопасности (ПК-2, ПК-3)
Форма проведения семинара – вопросно-ответная (предполагает совместное обсуждение вступденческой группе сформулированных в плане семинара проблем).
Информационная безопасность
Правовые основы информационной безопасности компании;
Коммерческая тайна компании;
Информационная безопасность и правоохранительные органы в законодательстве РФ;
Построение системы информационной безопасности компании;
Международные стандарты по информационной безопасности и концепции системного подхода кзащите информации.
IT - безопасность
Угрозы электронным информационным ресурсам;
Типовые сценарии НСД к электронным информационным ресурсам и защита от них;
Криптографическая защита информации;
Электронная цифровая подпись;
Защита от утери электронных информационных ресурсов;
Антивирусная защита информационных ресурсов;
Защита информации в автономных информационных системах;
Защита информационных сетей компании;
Защита информационных ресурсов от хакерских атак из Интернета;
Защита информации с использованием систем Honeypot;
Защита информации от продуктов-шпионов;
Анализ особенностей российского рынка IT- безопасности.

Тема 3. Кадровая безопасность (ПК-2, ПК-3)
Форма проведения семинара – вопросно-ответная (предполагает совместное обсуждение вступденческой группе сформулированных в плане семинара проблем).
Оперативная работа с кадрами;
Организация кадровой работы в компании;
Мотивация персонала компании;
Лояльность сотрудников компании;
Прием-увольнение сотрудников;
Применение полиграфа в тестировании сотрудников компании.
Порядок приобретения, хранения, ношения и применения оружия;
Психология безопасного поведения;
Основы невербального общения с людьми;
Различные способы получения конфиденциальной информации у сотрудников компании.

Тема 4. Экономическая безопасность корпорации. Экономическая паразитология (ПК-2, ПК-3)
Форма проведения семинара – вопросно-ответная (предполагает совместное обсуждение вступенческой группе сформулированных в плане семинара проблем).
Понятие «экономическая безопасность организации», «экономическая безопасность корпорации».Структура экономической безопасности корпорации.
Система и методы анализа и управления экономическими рисками. Виды экономических рисков.Методы оценки экономических рисков. Методы управления экономическими рисками.
Мошенничество: понятие, виды. Внутреннее и внешнее мошенничество. Признаки мошенничества.Выявление мошенничества. Основные способы устранения возможностей мошенничества.
Враждебное (недружественное) поглощение: понятие, виды, схемы. Основные цели враждебногопоглощения. Возможные варианты враждебного поглощения. Некоторые способы предотвращениявраждебного поглощения. Возможные способы защиты от начавшегося враждебного поглощения.Компании-агрессоры. Гринмейл.

Тема 5. Основы инженерно-технической безопасности (ПК-2, ПК-3)
Форма проведения семинара – вопросно-ответная (предполагает совместное обсуждение вступенческой группе сформулированных в плане семинара проблем).
Охранные мероприятия;
Противопожарная безопасность;
Системы охраны периметров;
Охранное телевидение;
Системы охранных сигнализаций;
Контрольно-пропускной режим в компании;
Биометрические системы распознавания личности.

Тема 6. Бизнес-разведка (ПК-2, ПК-3)
Форма проведения семинара – вопросно-ответная (предполагает совместное обсуждение вступенческой группе сформулированных в плане семинара проблем).
Бизнес-разведка: понятие, задачи, направления проведения.
Понятие «информационное задание» в бизнес-разведке.
Методы сбора информации, применяемые в бизнес-разведке.
Способы официального получения информации из государственных органов.
Сбор информации в сети Интернет.
Аналитические методы бизнес-разведки.

Тема 7. Организационные основы обеспечения корпоративной безопасности (ПК-2, ПК-3)
Форма проведения семинара – вопросно-ответная (предполагает совместное обсуждение вступенческой группе сформулированных в плане семинара проблем).
Организационные основы обеспечения корпоративной безопасности
Варианты организации обеспечения безопасности компании. Аутсорсинг безопасности. Цели изадачи обеспечения безопасности компании. Принципы организации и функционирования системыбезопасности компании. Средства обеспечения безопасности.
Служба безопасности компании: понятие, структура. Методы проверки работы службыбезопасности. Внутри объектовый режим. Пропускной режим. Система мер защиты компании.Управление системой безопасности компании.

7.3. Содержание самостоятельной работы

Тема 2. Основы обеспечения информационной безопасности (ПК-2, ПК-3) 1. Обзор дополнительной литературы. Изучение понятийного аппарата темы, лекционногоматериала, основной и дополнительной литературы, интернет-источников; 2. Подготовка к тесту
Тема 3. Кадровая безопасность (ПК-2, ПК-3) 1. Изучение понятийного аппарата темы, лекционного материала, основной и дополнительнойлитературы, интернет-источников; 2. Подготовка к тесту 3. Подготовка к выполнению индивидуального задания 1
Тема 4. Экономическая безопасность корпорации. Экономическая паразитология (ПК-2, ПК-3) 1. Изучение понятийного аппарата темы, лекционного материала, основной и дополнительнойлитературы, интернет-источников; 2. Подготовка к выполнению индивидуального задания 2
Тема 5. Основы инженерно-технической безопасности (ПК-2, ПК-3) 1. Изучение понятийного аппарата темы, лекционного материала, основной и дополнительнойлитературы, интернет-источников; 2. Подготовка к тесту 3. Подготовка к выполнению индивидуального задания 3
Тема 6. Бизнес-разведка (ПК-2, ПК-3) 1. Изучение понятийного аппарата темы, лекционного материала, глав, рекомендованныхучебников и дополнительных источников; 2. Выполнение индивидуального задания 4.
Тема 7. Организационные основы обеспечения корпоративной безопасности (ПК-2, ПК-3) 1. Изучение понятийного аппарата темы, лекционного материала, основной и дополнительнойлитературы, интернет-источников; 2. Выполнение задания по самостоятельной работе; 3. Подготовка к итоговому тесту Подготовка к экзамену.

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки кзачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
не предусмотрена

7.4. Электронное портфолио обучающегося
в портфолио работы не выкладываются

7.5. Методические рекомендации по выполнению контрольной работы
не предусмотрена

7.6 Методические рекомендации по выполнению курсовой работы
не предусмотрена

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

2. Ефимова Корпоративная безопасность. Курс лекций. Тема 3. Кадровая безопасность[Электронный ресурс]:. - Екатеринбург: [б. и.], 2025. - 1 – Режим доступа: https://libw.usue.ru/2025-08/30.mp4

3. Ефимова Корпоративная безопасность. Курс лекций. Тема 2. Основы обеспечения информационной безопасности [Электронный ресурс]:. - Екатеринбург: [б. и.], 2025. - 1 – Режим доступа: https://libw.usue.ru/2025-08/29.mp4

4. Ефимова Корпоративная безопасность. Курс лекций. Тема 1. Корпоративная безопасность:понятие, сущность, структура [Электронный ресурс]:. - Екатеринбург: [б. и.], 2025. - 1 – Режим доступа: https://libw.usue.ru/2025-08/28.mp4

5. Панарина М. М. Корпоративная безопасность. Управление рисками и комплаенс в эпохуцифровизации [Электронный ресурс]:учебное пособие для вузов. - Москва: Юрайт, 2025. - 181 –Режим доступа: https://urait.ru/bcode/559219

6. Бабурина О. Н. Экономическая безопасность [Электронный ресурс]:учебник и практикумдля вузов. - Москва: Юрайт, 2025. - 393 – Режим доступа: https://urait.ru/bcode/567606

Дополнительная литература:

2. Ефимова Корпоративная безопасность. Тесты. Тест 2. Основы обеспечения информационной безопасности [Электронный ресурс]:. - Екатеринбург: [б. и.], 2025. - 10 – Режим доступа: https://libw.usue.ru/2025-08a/49.docx

3. Яковлев В.М. Риск-ориентированный подход к модернизации корпоративного управления[Электронный ресурс]:Учебное пособие. - Москва: КноРус, 2024. - 142 – Режим доступа:https://book.ru/book/955150

4. Тарасов А. Н. Современные формы корпоративного мошенничества [Электронныйресурс]:практическое пособие. - Москва: Юрайт, 2025. - 320 – Режим доступа:https://urait.ru/bcode/560666

5. Ефимова Корпоративная безопасность. Тесты. Тест 1. Корпоративная безопасность:понятие, сущность, структура [Электронный ресурс]:. - Екатеринбург: [б. и.], 2025. - 9 – Режим доступа: https://libw.usue.ru/2025-08a/48.docx

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Astra Linux Common Edition. Договор №0417-ПО/2019 от 08.05.2019, Акт №Sk000343 от 24.05.2019 и Контракт № 35-У/2018 от 13.06.2018, Акт № УТ213 от 17.12.2018. Срок действия лицензии - без ограничения срока.

МойОфис стандартный. Соглашение № СК-281 от 7 июня 2017. Дата заключения - 07.06.2017. Срок действия лицензии - без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Консультант +. Договор № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

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

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к зачёту с оценкой

1. Корпоративная безопасность: определение, цель, задачи, составные элементы. Коммерческая тайна компании.
2. Объекты и субъекты обеспечения корпоративной безопасности. Варианты (уровни) субъектов обеспечения корпоративной безопасности.
3. Основные виды угроз корпоративной безопасности. Характеристика элементов системы корпоративной безопасности. Принципы построения корпоративной безопасности.
4. Правовые основы информационной безопасности компании; Информационная безопасность и правоохранительные органы в законодательстве РФ.
5. Построение системы информационной безопасности компании. Международные стандарты по информационной безопасности и концепции системного подхода к защите информации.
6. Угрозы электронным информационным ресурсам. Типовые сценарии НСД к электронным информационным ресурсам и защита от них.
7. Криптографическая защита информации. Электронная цифровая подпись. Защита от утери электронных информационных ресурсов.
8. Антивирусная защита информационных ресурсов. Защита информации в автономных информационных системах.
9. Защита информационных сетей компании. Защита информационных ресурсов от хакерских атак из Интернета.
10. Защита информации с использованием систем Honeypot. Защита информации от продуктов-шпионов.
11. Анализ особенностей российского рынка IT- безопасности.
12. Оперативная работа с кадрами. Организация кадровой работы в компании.
13. Мотивация персонала компании. Лояльность сотрудников компании. Прием-увольнение сотрудников.
14. Применение полиграфа в тестировании сотрудников компании. Различные способы получения конфиденциальной информации у сотрудников компании.
15. Порядок приобретения, хранения, ношения и применения оружия.
16. Психология безопасного поведения. Основы невербального общения с людьми.
17. Охранные мероприятия. Противопожарная безопасность. Системы охраны периметров. Охранное телевидение.
18. Системы охранных сигнализаций. Контрольно-пропускной режим в компании. Биометрические системы распознавания личности.

19. Понятие «экономическая безопасность организации», «экономическая безопасность корпорации». Структура экономической безопасности корпорации.

20. Система и методы анализа и управления экономическими рисками. Виды экономических рисков.

21. Методы оценки экономических рисков. Методы управления экономическими рисками.

22. Мошенничество: понятие, виды (внутреннее и внешнее), признаки. Выявление мошенничества. Основные способы устранения возможностей мошенничества.

23. Враждебное (недружественное) поглощение: понятие, виды, схемы. Основные цели враждебного поглощения.

24. Возможные варианты враждебного поглощения. Некоторые способы предотвращения враждебного поглощения.

25. Возможные способы защиты от начавшегося враждебного поглощения. Компании-агрессоры. Гринмейл.

26. Бизнес-разведка: понятие, задачи, направления проведения. Понятие «информационное задание» в бизнес-разведке. Методы сбора информации, применяемые в бизнес-разведке.

27. Способы официального получения информации из государственных органов. Сбор информации в сети Интернет. Аналитические методы бизнес-разведки.

28. Варианты организации обеспечения безопасности компании. Аутсорсинг безопасности. Цели и задачи обеспечения безопасности компании.

29. Принципы организации и функционирования системы безопасности компании. Средства обеспечения безопасности.

30. Служба безопасности компании: понятие, структура. Методы проверки работы службы безопасности.

31. Внутриобъектовый режим. Пропускной режим. Система мер защиты компании. Управление системой безопасности компании.

32. Система и методы анализа и управления экономическими рисками. Виды экономических рисков. Методы оценки экономических рисков.

Приложение 2
к рабочей программе

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачёту с оценкой

Задания закрытого типа

№ задания	Содержание задания	Компе-тенция
1	*Корпоративная безопасность – это:* а) объединение, сообщество лиц, объединяемых общностью профессиональных или сословных интересов; б) состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз; в) состояние защищенности жизненно важных интересов субъекта хозяйственной деятельности; г) состояние защищенности информационных ресурсов корпорации, достигаемое процессом защиты информации.	ПК-2
2	*Перечисленные причины способствуют появлению рисков и угроз. Среди них укажите общую, основную причину, по которой предприниматель вынужден принимать на себя риски:* а) неопределённость хозяйственной ситуации; б) отсутствие информации и случайность ситуаций; в) наличие внешних по отношению к стране угроз; г) наличие противодействия со стороны третьих лиц.	ПК-3
3	*Среди перечисленных четырёх факторов есть три, обуславливающие неопределённость хозяйственной ситуации. Укажите, какой из факторов оказался лишним:* а) информация (её отсутствие); б) недостаточность нормативно-правовой базы; в) случайность; г) противодействие со стороны третьих лиц.	ПК-3 ПК-2
4	*IT-безопасность корпорации – это:* а) состояние защищённости её инженерно-технической подсистемы; б) состояние защищённости от каналов утечки информации; в) состояние защищённости её информационных ресурсов; г) верны все варианты.	ПК-3
5	*Среди перечисленных назовите наиболее опасный вид базовых угроз корпоративной безопасности:* а) конкурентная борьба; б) организованная преступность; в) проявление человеческого фактора; г) техногенные и природные факторы.	ПК-3
6	*Назовите, на какие два вида подразделяют информационные ресурсы корпорации:* а) открытые; б) закрытые; в) частично закрытые; г) с ограниченным доступом.	ПК-2

7	*Назовите из перечисленных наиболее эффективный вариант обеспечения безопасности корпорации:* а) внешняя организация; б) совет безопасности + сотрудник; в) руководство корпорации; г) назначенный сотрудник безопасности.	ПК-2
8	*Назовите из перечисленных максимальный вариант с позиции обеспечения безопасности корпорации:* а) совет безопасности + сотрудник; б) служба безопасности корпорации; в) внешняя организация; г) руководство корпорации.	ПК-2
9	*Предметом интереса стратегического направления бизнес-разведки являются:* а) законодательство; конкурентная среда; новые технологии; ресурсы; б) новые технологии; ресурсы; изучение конкретной компании; в) законодательство; конкурентная среда; новые технологии; оперативные действия руководителя компании; г) изучение конкретной компании; изучение конкретного человека; изучение конкретной ситуации.	ПК-3
10	*Предметом интереса оперативного направления бизнес-разведки являются:* а) законодательство; конкурентная среда; новые технологии; ресурсы; б) новые технологии; ресурсы; изучение конкретной компании; в) законодательство; конкурентная среда; новые технологии; оперативные действия руководителя компании; г) изучение конкретной компании; изучение конкретного человека; изучение конкретной ситуации.	ПК-3

Задания открытого типа

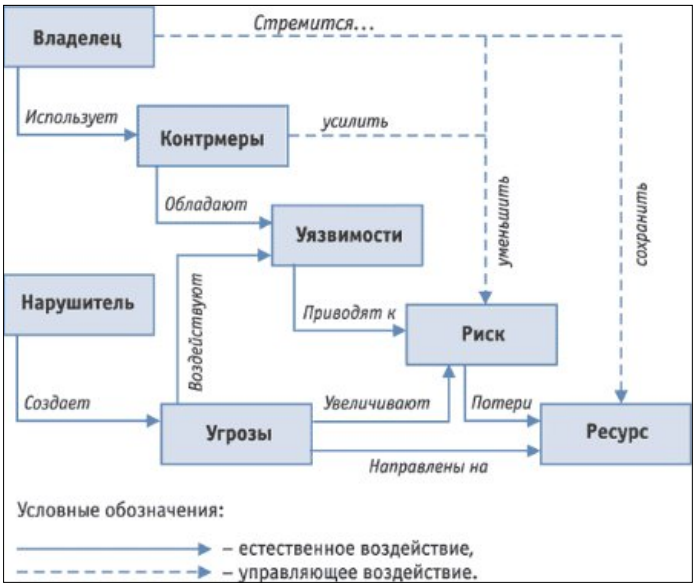
(кейс, расчетная или ситуационная задача, практико-ориентированное задание и др.)

№ задания	**Содержание задания**	**Компе-тенция**
1	Построение системы корпоративной безопасности индивидуально, зависит от особенностей, сферы деятельности корпорации/ организации, от специфики внешних и внутренних угроз. Универсальной системы корпоративной безопасности не предложено, но принято выделять в ней 8 основных элементов (подсистем). Назовите 8 подсистем корпоративной безопасности.	ПК-2
2	Назовите (дополните) два основных фактора построения корпоративной безопасности: _____ и _____ _____ на их нейтрализацию	ПК-2
3	Этот вид разведки ещё также называют конкурентной, деловой или корпоративной разведкой. Напишите, о какой разведке идёт речь?	ПК-2
4	Назовите методы определения коммерческой тайны (КТ) по их характеристикам:	ПК-2

	<table><tr><th>методы</th><th>характеристика</th></tr><tr><td>а) …</td><td>- коммерческой тайной признаётся всё, за исключением инфо, которая не таковой в соответствие с федеральным законом</td></tr><tr><td>б) …</td><td>- основан на необходимости, какая именно инфо составляет коммер аналогичных предприятий;</td></tr><tr><td>в) …</td><td>- анализируется, какая именно инфо может интересовать конкурентов.</td></tr><tr><td>г) …</td><td>- приглашение независимых экспертов для определения коммерческой тайны</td></tr></table>	
5	Допишите названия трёх основных нормативно-правовых актов РФ, содержащих понятие «коммерческая тайна»: № ____-ФЗ от _____ «название»; _____ кодекс РФ, статья ____ _____ кодекс РФ, статья ____	ПК-3
6	Среди перечисленных назовите 5 признаков, не относимых к коммерческой тайне: 1) коммерческая ценность; 2) государственная ценность; 3) недоступность; 4) охраняемость; 5) без уплаты госпошлины; 6) уплачивается госпошлина; 7) засекреченность; 8) неограниченность срока хранения; 9) ограниченность срока хранения; 10) требует официального признания.	ПК-3
7	Информационную безопасность обеспечивают в т.ч. правоохранительные органы. В 1997 г. с введением в действие УК РФ и установления уголовной ответственности за преступления в сфере компьютерной информации (гл. 28) и иных видов компьютерных преступлений, определённому органу управления «Р» придан статус оперативно-розыскного подразделения – специализированного органа дознания. Поскольку одновременно с новым УК РФ 1997 года действовал и старый Уголовно-процессуальный кодекс РСФСР 1964 года (действовал до конца 2001 г.), в новый были внесены поправки и изменения, которые касались и подследственности по преступлениям, находящимся в ведении Федеральной службы безопасности (ФСБ), так же находящейся в постоянной реорганизации. 7 октября 1998 г. Управление «Р» было преобразовано в Управление по борьбе с преступлениями в сфере высоких технологий (УБПСВТ), где в его структуре были выделены три подразделения, названия которых нужно дописать: 1. Отдел по борьбе с преступлениями в сфере … 2. Отдел по борьбе с преступлениями в сфере … 3. Отдел по борьбе с незаконным оборотом … …	ПК-3
8	В 2002 г. Управление БПСВТ было упразднено, а его штаты, структура и материально-техническое обеспечение были переданы … (*название органа согласно аббревиатуре БСТМ*) … при МВД России (напишите полное название органа).	ПК-3
9	Система информационной безопасности базируется на 9 основных принципах, для каждого из которых необходимо проведение определённых мероприятий. Заполните пропуски в таблице.	ПК-3

	<table><tr><th>Принцип</th><th>Мероприятия</th></tr><tr><td>1. Профилактика возможных угроз</td><td>А) выявление возможных угроз безопасности предприятия/организаци которых позволит разработать необходимые меры.</td></tr><tr><td>2. …</td><td>Б) меры по обеспечению безопасности, разрабатываемые на основе и действующих правовых актов.</td></tr><tr><td>3. Комплексное использование сил и средств</td><td>В) использование программы (плана работ) для обеспечения безопасн предприятия/организации, где каждый сотрудник должен участвовать компетенции.</td></tr><tr><td>4. Внешняя и внутренняя координация и взаимодействие</td><td>Г) усилия всех подразделений, служб предприятия, в т. ч. установлени необходимых контактов с внешними организациями, способными ока необходимое содействие в обеспечении безопасности предприятия;</td></tr><tr><td>5. Сочетание гласности с секретностью</td><td>Д) доведение информации до сведения персонала предприятия и обще допустимых пределах мер безопасности с целью предотвращения поте реальных угроз.</td></tr><tr><td>6. …</td><td>Е) вопросы обеспечения безопасности решаются сотрудниками на профессиональном уровне, а в необходимых случаях – специалистами профиля.</td></tr><tr><td>7. Экономическая целесообразность</td><td>Ж) стоимость финансовых затрат на обеспечение безопасности не дол оптимальный уровень, при котором теряется смысл их применения.</td></tr><tr><td>8. Плановая основа деятельности</td><td>З) деятельность по обеспечению безопасности предприятия на основе программы, подпрограмм обеспечения безопасности по основным его (экономическая, научно-техническая, экологическая, технологическая</td></tr><tr><td>9. Системность</td><td>И) учет всех факторов, оказывающих влияние на безопасность предпр включение в деятельность всех сотрудников, использование всех сил</td></tr></table>	
10	В системе корпоративной безопасности выделяют объекты её обеспечения, приведённые в таблице, где необходимо дописать название пропущенных. <table><tr><td rowspan="6">Объекты обеспечения корпоративной безопасности</td><td>1. Бизнес-процессы</td></tr><tr><td>2. Персонал</td></tr><tr><td>3. …</td></tr><tr><td>4. Материальные ценности</td></tr><tr><td>5. Информационные ресурсы</td></tr><tr><td>6. …</td></tr></table>	ПК-3
11	Коэффициент абсолютной ликвидности – показывает, какую часть текущей краткосрочной задолженности организация может погасить в ближайшее время за счет денежных средств и приравненных к ним финансовым вложениям. Коэффициент абсолютной ликвидности рассчитывают на основе показателей: *ФВ - фин. вложения (за искл. денежных);* *ДС - денежные средства;* *ЗС - заемные средства;* *КЗ – кредиторская задолженность;* *ПО - прочие обязательства.* Выберите правильный вариант расчёта коэффициента абсолютной ликвидности корпорации: а) $К_{ал}$ = ФВ+ДС / ЗС+КЗ+ПО б) $К_{ал}$ = ФВ+ДС / ЗС+КЗ – ПО	ПК-2
12	Коэффициент текущей ликвидности ($К_{тл}$) – позволяет установить, в какой кратности текущие активы покрывают краткосрочные обязательства. Его	ПК-2

<table>
<tr><td></td><td>рассчитывают на основе данных бухгалтерского баланса. Назовите показатель X в числителе расчёта данного коэффициента.
$К_{тл}$ = X / ЗС+КЗ+ПО, где
ЗС - заемные средства;
КЗ – кредиторская задолженность;
ПО - прочие обязательства;
X – это _____ активы
Дополните: $К_{тл}$ называют главным показателем _____ предприятия.</td><td></td></tr>
<tr><td>13</td><td>Коэффициент критической ликвидности ($К_{кл}$) – показывает какая часть краткосрочных обязательств организации может быть немедленно погашена за счёт денежных средств, средств в краткосрочных ценных бумагах, а также поступлений по расчетам.
Его можно рассчитать на основе следующих показателей бухгалтерского баланса:
ФВ – финансовые вложения;
ДС – денежные средства;
ДЗ – дебиторская задолженность;
ЗС – Заемные средства;
КЗ – кредиторская задолженность;
ПО – прочие обязательства.
Выберите правильный вариант расчёта коэффициента абсолютной ликвидности корпорации:
а) $К_{кл}$ = ФВ+ДС + ДЗ / ЗС+КЗ+ПО
б) $К_{кл}$ = ФВ – ДС + ДЗ / ЗС+КЗ+ПО
Нормальное значение коэффициента критической ликвидности не ниже ____.</td><td>ПК-2</td></tr>
<tr><td>14</td><td>Для понимания экономической безопасности корпорации/предприятия/организации рассчитывают показатели рентабельности. Назовите показатели рентабельности на основе приведённых в таблице их характеристик.
<table><tr><th>Характеристика показателя рентабельности</th><th>Показатель рентабельности</th></tr><tr><td>1. показывает отдачу каждого рубля, вложенного в оборотные активы –</td><td>…</td></tr><tr><td>2. характеризует сумму прибыли от продаж и приходящейся на каждый рубль затрат на производство и сбыт продукции –</td><td>…</td></tr><tr><td>3. показывает, сколько прибыли от продаж приходится на 1 рубль реализованной продукции –</td><td>…</td></tr><tr><td>4. характеризует эффективность и прибыльность использования всех активов предприятия –</td><td>…</td></tr></table></td><td>ПК-2</td></tr>
<tr><td>15</td><td>Для оценки безопасности корпорации рассчитывают показатель финансовой устойчивости (Ф_у), определяемый по состоянию излишка или недостатка источников средств для формирования запасов и затрат по данным бухгалтерского баланса. Полученный трёхкомпонентный показатель позволяет выявить степень финансовой устойчивости корпорации (предприятия) в соответствие со следующими четырьмя типами:
1) Фс>0, Фд>0, Фо>0
2) Фс<0, Фд>0, Фо>0
3) Фс<0, Фд<0, Фо>0
4) Фс<0, Фд<0, Фо<0</td><td>ПК-2</td></tr>
</table>

	Напишите типы состояний финансовой устойчивости в указанном порядке.	
16	Рассмотрите рисунок, где представлена модель Петренко С.А. Допишите – это модель построения системы _____ предприятия.  	ПК-3
17	Выделяют вербальные и невербальные средства общения людей. Психологи установили, что в процессе взаимодействия людей 60-80% коммуникаций осуществляется за счёт _____ средств выражения, и только 20-40% за счёт _____ средств выражения.	ПК-2
18	На рисунке представлены основные элементы системы корпоративной безопасности. Назовите элемент системы, который содержит наибольшую долю угроз для корпорации (предприятия). **Система корпоративной безопасности** Информационная | Кадровая | Экономическая | Инженерно-техническая | техническая | личная | IT	ПК-2
19	1. Выделяют две основные формы обучения персонала: на рабочем месте и вне рабочего места. По характеристикам определите форму обучения: более эффективной и боле затратной формой обучения персонала является _____; а обучение персонала _____ менее затратно и облегчает вхождение работников в учебный процесс.	ПК-3
20	В коммерческих структурах сложились разные уровни (варианты) субъектов обеспечения безопасности – тех, кто непосредственно занимается обеспечением безопасности корпорации. Допишите название субъектов безопасности в вариантах 1 и 6.	ПК-3

	Субъекты обеспечения корпоративной безопасности **Вариант:** / **Обеспечением безопасности корпорации занимается:** 1 вариант (уровень): — …. 2 вариант (уровень) — сотрудник, у которого есть иные должностные обязанности или ещё это называют «работа по совместительству»; 3 вариант (уровень) — сотрудник, у которого эта работа входит в основные должностные обязанности («отдельная должность») 4 вариант (уровень) — совет по безопасности (совещательный орган) + сотрудник, у которого эта работа входит в основные должностные обязанности 5 вариант (уровень) — внешняя организация (или «абонентское обслуживание» по вопросам безопасности) 6 вариант (уровень) — …. 7 вариант (уровень) — смешанный, из любых первых пяти вариантов, с учётом характера деятельности корпорации.	
21	1. Выделяют две группы мотивирующих факторов: усиливающих лояльность и ослабляющих лояльность сотрудников. Определите: формальный (недемократичный) стиль руководства способствует ослаблению или усилению лояльности сотрудников? 2.	ПК-3
22	На российском рынке IT-безопасности и компьютерной безопасности велика роль государства, где оно регулирует его с помощью 3 основных механизмов, среди которых нужно назвать один из пропущенных: - лицензирования участников рынка, - _____ продукции, выпускаемой на этот рынок, - контроля ввоза-вывоза средств защиты компьютерной инфо.	ПК-3
23	Выделяют разные методы определения коммерческой тайны корпорации, среди которых: *тотальный, плагиаторский, аналитический, экспертный*. Какой из названных методов является наиболее эффективным, но и самым дорогостоящим?	ПК-3
24	Выделяют методы определения коммерческой тайны корпорации: *тотальный, плагиаторский, аналитический, экспертный* Назовите метод, который основан на выяснении, какую именно информацию считают коммерческой тайной аналогичные профильные компании, для определения собственной коммерческой тайны.	ПК-3
25	Аналитическая работа в бизнес-разведке обычно строится по двум направлениям: 1. анализ деятельности конкурента, партнера, контрагента; 2. анализ конкурентной среды.	ПК-2

Определите направления бизнес-разведки под буквой А и Б.

	Направление бизнес-разведки	*Методы анализа информации в бизнес-разведке*
А	???	синтез, аналогии; исключения; причинно-следственных связей; технический анализ; контент-анализ
Б	???	пять сил М. Портера; Due Diligence; SWOT; диверсионный

<table>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td>анализ; экспертный.</td></tr>
</table>
</td><td></td></tr>
<tr><td>26</td><td>Назовите пропущенные в таблице подсистемы (элементы) корпоративной безопасности.
<table>
<tr><td rowspan="9">Система корпоративной безопасности</td><td>Подсистемы</td><td>Характеристика подсистем:</td></tr>
<tr><td>Информационная</td><td>- состояние защищенности ее информационных ресурсов, котор процессом защиты информации.</td></tr>
<tr><td>???</td><td>- состояние защищённости корпорации от противоправных дейс разглашения информации, некомпетентных действий человека</td></tr>
<tr><td>Экономическая</td><td>- состояние защищённости бизнес-процессов организации</td></tr>
<tr><td>Инженерно-техническая</td><td>- состояние защищённости инженерно-технического оборудован и принадлежащей ей территории</td></tr>
<tr><td>Техническая</td><td>- состояние защищённости от каналов утечки информации</td></tr>
<tr><td>???</td><td>- состояние защищённости первых лиц корпорации в физическо юридическом и психологическом аспектах</td></tr>
<tr><td>IT-безопасность</td><td>- состояние защищённости информационных ресурсов корпора представленной в электронном виде.</td></tr>
</table>
</td><td>ПК-3</td></tr>
<tr><td>27</td><td>Применение наклеек (табличек) с содержанием «Охраняется полицией», «Ведётся видеонаблюдение», «Во дворе злая собака», муляжей видеокамер и т.п. является принципом _____ воздействия на потенциального нарушителя.</td><td>ПК-3</td></tr>
<tr><td>28</td><td>Угрозы безопасности организации классифицируются на постоянные и временные.
Выберите среди перечисленных примеров угроз те, которые относят к постоянным:
1) воровство товаров в магазинах; 2) изменение законодательства; 3) появление новых товаров и услуг; 4) передел сфер влияния на рынке; 5) невозврат потребительских кредитов.</td><td>ПК-3</td></tr>
<tr><td>29</td><td>Выделяют три уровня мошенничества (злоупотреблений) сотрудниками:
1) уровень 1 «мелкие разовые хищения»;
2) уровень 2 «систематические хищения среднего размера»;
3) уровень 3 «внутреннее предпринимательство»;
Определите уровень, для которого применяется такой способ борьбы, как увольнение старого персонала и найм новых сотрудников?</td><td>ПК-3</td></tr>
<tr><td>30</td><td>Экономическая безопасность – это одна из подсистем (элемент) корпоративной безопасности, обеспечивающий безопасность её бизнес-процессов. Обеспечение экономической безопасности корпорации предполагает проведение бизнес-разведки, проведение которой включает _____ (допишите).</td><td>ПК-3</td></tr>
</table>