МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета математики и компьютерных наук имени профессора Н. И. Червякова
Гробова Т. А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
«Информационная безопасность»

Направление подготовки	02.04.01 Математика и компьютерные науки
Профиль	Искусственный интеллект в кибербезопасности
Год начала обучения	2026
Форма обучения	очная
Реализуется в 1 семестре	

Введение

1. Назначение: Фонд оценочных средств предназначен для обеспечения методической основы для организации и проведения текущего контроля по дисциплине «Информационная безопасность». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информации о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.

2. ФОС является приложением к программе дисциплины «Информационная безопасность»

3. Разработчик: кафедры вычислительной математики и кибернетики.

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель

Бабенко М. Г. заведующий кафедрой вычислительной математики и кибернетики.

Члены комиссии:

Пелешенко В.С. доцент кафедры вычислительной математики и кибернетики.

Пелешенко Т. А. доцент кафедры вычислительной математики и кибернетики.

Представитель организации-работодателя Корниенко С. А. начальник управления филиала ФГУП «Главный радиочастотный центр» в Южном и Северо-Кавказском федеральных округах

Экспертное заключение: фонд оценочных средств соответствует образовательной программе по направлению подготовки 02.04.01 Математика и компьютерные науки профиль «Искусственный интеллект в кибербезопасности» и рекомендуется для проведения текущего контроля успеваемости и промежуточной аттестации студентов.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенци(ий),			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ПК-4 Способен проводить патентные исследования, определять формы и методы правовой охраны и защиты прав на результаты интеллектуальной деятельности, распоряжаться правами на них для решения задач в области развития науки, техники и технологии				
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-1. ПК-4.* Осуществляет рациональный выбор по методам защиты прав на интеллектуальную собственность;	Не осуществляет Рациональный выбор по методам защиты прав на интеллектуальную собственность;	С трудом осуществляет рациональный выбор по методам защиты прав на интеллектуальную собственность;	С ошибками осуществляет рациональный выбор по методам защиты прав на интеллектуальную собственность	Осуществляет рациональный выбор по методам защиты прав на интеллектуальную собственность
ИД-2. ПК-4. Осуществляет патентные исследования в области вычислительной техники и систем связи.	Не осуществляет патентные исследования в области вычислительной техники и систем связи.	С трудом осуществляет патентные исследования в области вычислительной техники и систем связи.	С ошибками осуществляет патентные исследования в области вычислительной техники и систем связи.	Осуществляет патентные исследования в области вычислительной техники и систем связи

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения очная/заочная/очно-заочная	
1.	информационная безопасность — это защита информации от несанкционированного доступа, утраты или повреждения. В широком смысле она охватывает комплекс мер, направленных на защиту данных, систем и сетей от угроз, включая физическую безопасность, управление рисками и соблюдение правовых норм	Дайте понятие информационной безопасности в узком и широком смысле слова.	ПК-4
2.	Риски — это вероятность наступления неблагоприятных событий, которые могут негативно повлиять на достижение целей. Существует несколько видов рисков, включая финансовые, операционные, стратегические и репутационные, каждый из	Дайте определение рисков и охарактеризуйте их виды.	ПК-4

	которых требует особого подхода к управлению.		
3.	Угрозы — это потенциальные события или действия, которые могут причинить вред объектам защиты, таким как информация, системы или ресурсы. Виды угроз включают физические (например, стихийные бедствия), технические (вирусы, хакерские атаки), социальные (мошенничество, внутренние угрозы) и экологические (потеря ресурсов, загрязнение).	Дайте определение угроз и охарактеризуйте их виды.	ПК-4
4.	Основные способы нарушения информационной безопасности включают вирусные атаки, фишинг (мошенничество с целью получения конфиденциальной информации), несанкционированный доступ к системам и утечку данных. Также распространены атаки типа	Охарактеризуйте основные наиболее распространенные способы нарушения информационной безопасности.	ПК-4

	"отказ в обслуживании" (DDoS), которые направлены на перегрузку систем, и использование уязвимостей программного обеспечения.		
5.	Процесс обеспечения информационной безопасности на предприятиях включает оценку рисков, разработку политики безопасности и внедрение технических мер защиты. Также важными аспектами являются обучение сотрудников и мониторинг систем для своевременного выявления угроз и реагирования на инциденты. Эти шаги помогают защитить данные и минимизировать потенциальные риски.	Охарактеризуйте процесс обеспечения собственной информационной безопасности на предприятиях.	ПК-4
6.	Основные международные организации в сфере информационной безопасности включают ISO, NIST, ITU и ENISA. ISO разрабатывает стандарты управления информационной	Укажите основные международные организации, действующие в сфере информационной безопасности, и укажите решаемые ими задачи.	ПК-4

	безопасностью, NIST создает руководства для кибербезопасности, ITU устанавливает нормы для защиты коммуникационных технологий, а ENISA поддерживает страны ЕС в повышении уровня кибербезопасности и реагирования на инциденты. Эти организации способствуют формированию лучших практик и стандартов в области защиты информации.		
7.	Крупные международные профессиональные организации характеризуются глобальным представительством, объединяя экспертов из разных стран для обмена знаниями. Они разрабатывают стандарты и сертификации, а также предлагают образовательные ресурсы и платформы для сетевого взаимодействия, что способствует развитию и	Опишите отличительные особенности крупных международных профессиональных (отраслевых) организаций (объединений).	ПК-4

	поддержанию высоких профессиональных стандартов в отрасли.		
8.	Международный союз электросвязи (ITU) назначен для координации глобальных телекоммуникационных стандартов и ресурсов, а также для содействия развитию и доступности связи в мире. Его структура включает Генеральную ассамблею, Советы и различные сектора, отвечающие за радиосвязь, стандартизацию и развитие. Сфера деятельности ITU охватывает вопросы, связанные с регулированием частотного спектра, разработкой стандартов и поддержкой инноваций в области связи и информационных технологий.	Назначение, структура и сфера деятельности International Telecommunication Union (ITU) – Международного союза электросвязи.	ПК-4
9.	Международный союз электросвязи (ITU) отвечает за координацию глобальных телекоммуникационных	Назначение, структура и сфера деятельности International Telecommunication Union (ITU) – Международного союза электросвязи.	ПК-4

	стандартов и развитие доступности связи. Его структура включает Генеральную ассамблею, Советы и специализированные сектора, которые занимаются радиосвязью, стандартизацией и развитием. Сфера деятельности ITU охватывает регулирование частотного спектра, разработку стандартов и поддержку инноваций в области информационных технологий.		
10.	Система управления информационной безопасностью (СУИБ) предприятия — это комплекс организационных, технических и правовых мер, направленных на защиту информации от несанкционированного доступа, утраты и других угроз. Состав СУИБ включает политику информационной безопасности, процедуры, технологии защиты, а также	Дайте определение системы управления информационной безопасностью (СУИБ) предприятия, приведите её состав и цели создания.	ПК-4

	обучение персонала. Основные цели создания СУИБ — обеспечение конфиденциальности, целостности и доступности информации, а также минимизация рисков и соблюдение законодательных требований.		
11.	Основные этапы разработки системы управления информационной безопасностью (СУИБ) включают анализ рисков, разработку политики безопасности, проектирование и внедрение защитных мер, обучение персонала и мониторинг системы. Успех разработки зависит от поддержки руководства, вовлеченности сотрудников и соблюдения законодательных требований.	Основные этапы и условия разработки СУИБ.	ПК-4
12.	Этап инвентаризации активов компании в разработке СУИБ заключается в выявлении и	Охарактеризуйте этап разработки СУИБ: Инвентаризация активов компании.	ПК-4

	классификации всех информационных активов, включая данные, оборудование и программное обеспечение. Это помогает определить их ценность и уязвимости, что является основой для дальнейшего анализа рисков и разработки мер защиты. Тщательная инвентаризация обеспечивает понимание того, какие ресурсы нуждаются в защите и какие угрозы им могут угрожать.		
13.	Этап категорирования активов компании в разработке СУИБ включает классификацию информационных активов по уровням важности и чувствительности. Это позволяет определить, какие активы требуют повышенной защиты и какие риски могут им угрожать. Правильное категорирование помогает сосредоточить усилия на защите наиболее критичных ресурсов.	Охарактеризуйте этап разработки СУИБ: Категорирование активов компании.	ПК-4

14.	Этап оценки защищенности информационной системы в разработке СУИБ включает анализ существующих мер безопасности и уязвимостей системы. Это позволяет выявить слабые места, которые могут быть exploited, и оценить уровень защиты активов. Результаты оценки помогают в разработке рекомендаций по улучшению безопасности и минимизации рисков.	Охарактеризуйте этап разработки СУИБ: Оценка защищенности информационной системы.	ПК-4
15.	Этапы определения политики безопасности предприятия включают анализ текущих угроз и уязвимостей, а также оценку бизнес-потребностей и требований законодательства. На основе собранной информации разрабатываются основные принципы и правила, регулирующие защиту информации и активов. Завершающим этапом является утверждение и внедрение политики, а	Охарактеризуйте этапы определения политики безопасности предприятия.	ПК-4

	также регулярный мониторинг и обновление для обеспечения ее актуальности.		
16.	Организационная структура менеджмента обеспечения информационной безопасности предприятия обычно включает несколько уровней, начиная с высшего руководства, которое определяет стратегию и политику безопасности. На среднем уровне располагаются специалисты по информационной безопасности, отвечающие за реализацию и контроль мер защиты, а на оперативном уровне — команды, занимающиеся повседневными задачами и реагированием на инциденты. Эта структура обеспечивает эффективное взаимодействие и распределение обязанностей для защиты информационных активов предприятия.	Опишите организационную структуру менеджмента обеспечения информационной безопасности предприятия.	ПК-4

17.	Основные функции отдела информационной безопасности предприятия включают разработку и внедрение стратегий защиты информации, мониторинг и анализ угроз, а также управление инцидентами. Кроме того, отдел отвечает за обучение сотрудников и проведение аудитов для обеспечения соблюдения норм и стандартов безопасности. Эти функции помогают защитить данные и минимизировать риски для организации.	Основные функции отдела информационной безопасности предприятия.	ПК-4
18.	Сценарий анализа информационных рисков компании включает идентификацию активов, уязвимостей и потенциальных угроз, а также оценку вероятности и последствий их реализации. Затем проводится анализ существующих мер защиты и разработка рекомендаций по улучшению безопасности. В результате формируется план действий	Сценарий анализа информационных рисков компании.	ПК-4

	для минимизации рисков и повышения устойчивости компании к инцидентам.		
19.	Политика безопасности предприятия — это документ, который определяет основные принципы, цели и меры по защите информации и ресурсов компании. Она служит основой для управления рисками, устанавливает правила поведения для сотрудников и определяет процедуры реагирования на инциденты, обеспечивая тем самым защиту данных и минимизацию угроз.	Дайте определение и поясните смысл политики безопасности предприятия.	ПК-4
20.	Схема управления безопасностью информационных технологий включает оценку рисков, разработку политик и процедур, контроль доступа, обучение сотрудников, мониторинг и аудит, а также реагирование на инциденты. Эти элементы работают вместе для обеспечения	Приведите схему управления безопасностью информационных технологий.	ПК-4

	комплексной защиты информации и ресурсов компании.		
21.	Основные этапы управления безопасностью информационных технологий включают оценку рисков для выявления уязвимостей, разработку и внедрение политик безопасности, а также обучение сотрудников. Далее следует мониторинг и аудит для проверки эффективности мер безопасности, а также реагирование на инциденты для минимизации последствий угроз	Поясните основные этапы управления безопасностью информационных технологий.	ПК-4
22.	Процедура оценки общего уровня риска при управлении безопасностью информационных технологий включает идентификацию активов и угроз, анализ уязвимостей и оценку вероятности возникновения инцидентов. Затем проводится оценка потенциальных последствий для бизнеса,	Опишите процедуру оценки общего уровня риска при управлении безопасностью информационных технологий.	ПК-4

	что позволяет определить общий уровень риска и приоритизировать меры по его снижению.		
23.	Оценка важности информационных технологий для функционирования организации начинается с анализа бизнес-процессов и идентификации ключевых IT-активов, которые поддерживают эти процессы. Затем оцениваются последствия возможных сбоев в работе IT-систем, что помогает определить их критичность для достижения бизнес-целей. На основе этой информации разрабатываются стратегии управления рисками и обеспечения непрерывности бизнеса.	Порядок оценки важности информационные технологий для функционирования организации.	ПК-4
24.	Департамент информационной безопасности предприятия (ДИБП) отвечает за защиту информационных активов и данных от угроз и	Дайте определение и раскройте задачи, решаемые департаментом информационной безопасности предприятия (ДИБП).	ПК-4

	инцидентов. Его основные задачи включают разработку и внедрение политик безопасности, мониторинг и анализ рисков, обучение сотрудников, а также реагирование на инциденты и обеспечение соблюдения нормативных требований. Это позволяет минимизировать риски и защитить репутацию организации.		
25.	Функции ДИБП, связанные с формированием и поддержкой политики информационной безопасности, включают разработку стратегий и стандартов безопасности, а также регулярный мониторинг их выполнения. ДИБП также отвечает за документальное обеспечение, что подразумевает создание и актуализацию необходимых инструкций, регламентов и отчетности по вопросам информационной	Опишите функции ДИБП, связанные с формированием, поддержкой и документальным обеспечением политики информационной безопасности предприятия.	ПК-4

	безопасности. Эти действия способствуют созданию четкой структуры управления безопасностью и повышению осведомленности сотрудников.		
26.	Функции ДИБП, связанные с внедрением средств защиты информации, включают выбор и интеграцию технологий для обеспечения безопасности данных, таких как антивирусное ПО, системы обнаружения вторжений и шифрование. ДИБП также проводит оценку эффективности этих средств и осуществляет их регулярное обновление и поддержку. Это помогает защитить информацию от несанкционированного доступа и других угроз.	Опишите функции ДИБП, с внедрением средств защиты информации.	ПК-4
27.	Функции ДИБП, связанные с администрированием информационных систем и систем защиты информации, включают настройку, мониторинг и	Опишите функции ДИБП, связанные с администрированием информационных систем и систем защиты информации.	ПК-4

	управление безопасностью IT-инфраструктуры. ДИБП также отвечает за управление доступом пользователей, обновление программного обеспечения и реагирование на инциденты безопасности. Эти действия обеспечивают надежную защиту данных и поддерживают стабильность работы информационных систем.		
28.	Аудит состояния информационной безопасности предприятия — это систематическая проверка и оценка существующих мер безопасности, процессов и политики для выявления уязвимостей и соответствия требованиям. Виды аудита включают внутренний аудит, проводимый самой организацией, и внешний аудит, осуществляемый независимыми экспертами. Также различают соответствующий аудит, который фокусируется на соответствии стандартам, и	Дайте определение аудита состояния информационной безопасности предприятия. Охарактеризуйте их виды.	ПК-4

	технический аудит, который анализирует технические аспекты защиты информации.		
29.	Цели аудита состояния информационной безопасности предприятия заключаются в выявлении уязвимостей, оценке эффективности существующих мер безопасности и обеспечении соответствия нормативным требованиям. Стратегическая задача аудита состоит в формировании комплексного подхода к управлению рисками, что позволяет минимизировать угрозы и защитить активы организации. Это способствует повышению общего уровня безопасности и устойчивости бизнеса.	Опишите цели и стратегическую задачу аудита состояния информационной безопасности предприятия.	ПК-4
30.	Организации, проводящие внешний аудит состояния информационной безопасности, должны обладать соответствующей	Опишите требования к организациям, осуществляющим внешний аудит состояния информационной безопасности предприятия.	ПК-4

	квалификацией и опытом в области информационной безопасности, а также быть независимыми от проверяемой организации. Они должны следовать установленным стандартам и методологиям аудита, обеспечивая объективность и прозрачность процесса. Кроме того, важна наличие сертификатов и лицензий, подтверждающих их компетентность в данной области.		
31.	Основные этапы аудита состояния информационной безопасности предприятия включают подготовительный этап, оценку текущего состояния безопасности, анализ уязвимостей и формирование рекомендаций. На подготовительном этапе определяются цели и задачи аудита, затем проводится сбор информации и оценка существующих мер безопасности. После анализа уязвимостей	Основные этапы аудита состояния информационной безопасности предприятия и их характеристика.	ПК-4

	формируется отчет с рекомендациями по улучшению системы безопасности и устранению выявленных недостатков.		
32.	Процесс анализа действующей на предприятии политики безопасности включает оценку ее соответствия актуальным требованиям и стандартам, а также выявление слабых мест и недостатков. Анализируется, насколько эффективно реализуются установленные меры безопасности и соблюдаются процедуры. Результаты анализа помогают определить области для улучшения и обновления политики безопасности.	Охарактеризуйте процесс анализа действующей на предприятии политики безопасности.	ПК-4
33.	Процесс изучения действующих информационных ресурсов предприятия включает инвентаризацию всех активов, оценку их состояния и уровня	Охарактеризуйте процесс изучения (проверки) действующих информационных ресурсов предприятия.	ПК-4

	безопасности. Также проводится анализ доступа к ресурсам и их использования, чтобы выявить уязвимости и риски. Результаты проверки помогают оптимизировать управление информационными ресурсами и повысить их защиту.		
34.	Программная поддержка реализации политики информационной безопасности обеспечивается через использование специализированных программных продуктов, которые автоматизируют процессы мониторинга, управления доступом, шифрования данных и защиты от угроз. Основные функции таких программ включают выявление и предотвращение вторжений, управление инцидентами, аудит безопасности и соблюдение нормативных требований. Это помогает обеспечить	Каким образом обеспечивается программная поддержка реализации политики информационной безопасности и основные функции специальных программных продуктов.	ПК-4

	защиту информации и минимизировать риски для предприятия.		
35.	Виды программных средств поддержки реализации политики информационной безопасности включают антивирусные программы, системы предотвращения вторжений (IPS), инструменты управления доступом и шифрования данных. Эти средства обеспечивают защиту от угроз, контроль прав пользователей и защиту конфиденциальной информации. Их использование способствует созданию безопасной информационной среды в организации.	Виды программных средств поддержки реализации политики информационной безопасности.	ПК-4
36.	Сборники программных средств поддержки реализации политики информационной безопасности представляют собой комплексы инструментов, предназначенных для	Дайте характеристику сборников - программных средств поддержки реализации политики информационной безопасности.	ПК-4

	защиты информации и управления рисками. Они включают антивирусные решения, системы мониторинга и управления доступом, а также инструменты для шифрования данных. Такие сборники помогают организациям эффективно реализовывать меры безопасности и обеспечивать защиту критически важной информации.		
37.	Программный продукт «COBRA» представляет собой комплексное решение для управления информационной безопасностью, которое включает инструменты для мониторинга, анализа и реагирования на инциденты. Его базовый модуль обеспечивает автоматизацию процессов управления безопасностью, включая управление политиками, оценку рисков и аудит. «COBRA» помогает организациям	Дайте характеристику программного продукта «COBRA» и его базового модуля.	ПК-4

	эффективно защищать свои активы и соответствовать требованиям законодательства.		
38.	Отчет о состоянии информационной безопасности программного продукта «COBRA» включает разделы, описывающие текущие угрозы, уязвимости системы и результаты проведенных аудитов. Он также содержит анализ инцидентов безопасности, оценку эффективности мер защиты и рекомендации по улучшению безопасности. Такой отчет помогает руководству принимать обоснованные решения для повышения уровня информационной безопасности в организации.	Структура и краткое содержание отчета о состоянии информационной безопасности программного продукта «COBRA».	ПК-4
39.	Программный комплекс управления политикой информационной безопасности компании «КОНДОР+» предназначен для автоматизации	Дайте характеристику программного комплекса управления политикой информационной безопасности компании «КОНДОР+».	ПК-4

	процессов создания, внедрения и контроля соблюдения политик безопасности. Он обеспечивает централизованное управление документами, оценку рисков и мониторинг соответствия, что помогает организациям минимизировать угрозы и повысить уровень защиты информации. Комплекс также включает инструменты для обучения сотрудников и повышения их осведомленности в области безопасности.		
40.	Инцидент в сфере информационной безопасности — это любое событие, которое нарушает или угрожает целостности, конфиденциальности или доступности информации. Причинами инцидентов могут быть как внешние факторы, такие как кибератаки и вирусы, так и внутренние, например, ошибки сотрудников или недостатки в системах	Дайте понятие инцидента в сфере информационной безопасности и причины его обуславливающие.	ПК-4

	безопасности. Эффективное управление инцидентами помогает минимизировать последствия и улучшить защиту информации.		
41.	Организационные процедуры реагирования на инциденты (регламенты) представляют собой набор заранее определенных действий и шагов, которые необходимо предпринять в случае возникновения инцидента в сфере информационной безопасности. Они включают в себя идентификацию инцидента, его оценку, устранение последствий, восстановление систем и анализ для предотвращения повторения. Эти процедуры помогают обеспечить слаженное и эффективное реагирование, минимизируя ущерб и восстанавливая нормальное функционирование организации.	Охарактеризуйте организационные процедуры (регламенты) реагирования на инциденты.	ПК-4

42.	Этап обнаружения нападения при реагировании на инциденты включает в себя выявление и подтверждение факта нарушения безопасности, используя различные инструменты мониторинга и анализа данных. На этом этапе важна быстрая и точная оценка угрозы, чтобы минимизировать потенциальный ущерб. Эффективное обнаружение позволяет оперативно реагировать и инициировать последующие действия по устранению инцидента.	Дайте характеристику этапа обнаружение нападения при реагировании на инциденты.	ПК-4
43.	Этап локализации нападения при реагировании на инциденты включает в себя изоляцию затронутых систем и ресурсов для предотвращения дальнейшего распространения угрозы. На этом этапе важно определить границы инцидента и ограничить доступ к уязвимым	Дайте характеристику этапа локализация нападения при реагировании на инциденты.	ПК-4

	компонентам, чтобы защитить остальные части инфраструктуры. Эффективная локализация способствует минимизации ущерба и подготовке к последующим действиям по устранению инцидента.		
44.	Предпосылки для формирования рынка услуг по обеспечению информационной безопасности включают рост числа кибератак и утечек данных, что создает потребность в защите информации. Также важным фактором является ужесточение законодательства и нормативных требований, требующих от организаций соблюдения стандартов безопасности. В результате компании начинают инвестировать в специализированные решения и услуги для защиты своих активов и репутации.	Охарактеризуйте предпосылки для формирования рынка различных услуг по обеспечению информационной безопасности.	ПК-4

45.	Достоинства применения аутсорсинга в сфере информационной безопасности включают доступ к высококвалифицированным специалистам и современным технологиям, что может снизить затраты и повысить уровень защиты. Однако недостатками являются возможные риски утечки конфиденциальной информации и потеря контроля над внутренними процессами. Кроме того, зависимость от внешних поставщиков может привести к задержкам в реагировании на инциденты.	Достоинства и недостатки применения аутсорсинга в сфере информационной безопасности.	ПК-4
46.	Основные виды услуг, которые могут быть переданы на аутсорсинг в сфере информационной безопасности, включают управление угрозами и инцидентами, мониторинг безопасности и реагирование на инциденты. Также часто	Основные виды услуг, которые могут быть переданы на аутсорсинг в сфере информационной безопасности.	ПК-4

	аутсорсируются услуги по проведению аудитов безопасности, тестированию на проникновение и обучению сотрудников. Эти услуги помогают организациям эффективно защищать свои данные и инфраструктуру без необходимости содержать внутреннюю команду.		
47.	Услуга по реагированию на инциденты в сфере информационной безопасности включает в себя быструю идентификацию, анализ и устранение угроз, а также восстановление нормального функционирования систем после инцидента. Команда специалистов проводит расследование для определения причин нарушения и разработку мер по предотвращению повторения подобных ситуаций. Это позволяет минимизировать ущерб и восстановить доверие к	Дайте характеристику услуги по реагированию на инциденты (нарушения информационной безопасности).	ПК-4

	системам безопасности организации.		
48.	Услуга аудита информационной безопасности включает в себя систематическую оценку и анализ политики, процедур и технологий безопасности организации. Аудит помогает выявить уязвимости, несоответствия и риски, а также предоставляет рекомендации для улучшения защиты данных и систем. Это важный инструмент для обеспечения соответствия стандартам и повышения общего уровня безопасности.	Дайте характеристику услуги аудита информационной безопасности.	ПК-4
49.	Услуга проверки защищенности и надежности отдельных элементов информационной инфраструктуры направлена на оценку уязвимостей и потенциальных рисков в системах, приложениях и сетях. Она включает в себя	Дайте характеристику услуги проверки защищенности и надежности отдельных элементов информационной инфраструктуры.	ПК-4

	тестирование на проникновение, анализ конфигураций и оценку защиты данных, что позволяет выявить слабые места и повысить уровень безопасности. Результаты проверки помогают организациям улучшить свои меры защиты и минимизировать угрозы.		
50.	Основные стадии процесса страхования информационных рисков включают идентификацию рисков, их оценку, выбор подходящей стратегии страхования и заключение договора. На первой стадии анализируются возможные угрозы и уязвимости, затем оценивается вероятность и последствия этих рисков. После этого выбираются страховые продукты, которые обеспечат защиту, и подписывается контракт с страховой компанией.	Основные стадии процесса страхования информационных рисков.	ПК-4
51.	Основные направления внешней организационной работы корпорации	Основные направления внешней организационной работы корпорации Microsoft в сфере информационной безопасности.	ПК-4

	Microsoft в сфере информационной безопасности включают сотрудничество с правительственными учреждениями и международными организациями для разработки стандартов безопасности, а также активное участие в инициативе по обмену информацией о киберугрозах. Microsoft также проводит образовательные программы и тренинги для клиентов и партнеров, чтобы повысить осведомленность о безопасности. Кроме того, компания активно развивает технологии защиты данных и реагирования на инциденты.		
52.	Методология Жизненного цикла безопасной разработки Microsoft Security Development Lifecycle (SDL) представляет собой структурированный	Сущность методологии Жизненного цикла безопасной разработки – Microsoft Security Development Lifecycle (SDL).	ПК-4

	процесс, который интегрирует практики безопасности на всех этапах разработки программного обеспечения. Она включает в себя планирование, проектирование, разработку, тестирование и развертывание, с акцентом на выявление и устранение уязвимостей на ранних стадиях. Цель SDL — обеспечить создание более безопасных продуктов и минимизировать риски для пользователей.		
53.	Программа построения партнерских отношений Microsoft Security Partners направлена на сотрудничество с независимыми компаниями для усиления кибербезопасности и обмена знаниями. Партнеры получают доступ к ресурсам, инструментам и поддержке Microsoft, что позволяет им разрабатывать и предлагать более эффективные решения по безопасности. Эта	Сущность программы построения партнерских отношений с различными независимыми компаниями Microsoft Security Partners.	ПК-4

	программа способствует созданию экосистемы, в которой компании могут совместно работать над защитой от киберугроз.		
54.	Программа обеспечения безопасности правительств (Government Security Program, GSP) от Microsoft предназначена для поддержки правительственных организаций в обеспечении защиты данных и соблюдении стандартов безопасности. Она предоставляет доступ к информации о безопасности продуктов Microsoft, а также к инструментам и ресурсам для оценки и управления рисками. GSP способствует повышению доверия к технологиям Microsoft в государственных учреждениях и помогает им эффективно противостоять киберугрозам.	Сущность программы обеспечения безопасности правительств Government Security Program (GSP).	ПК-4
55.	Централизованная сертификация программных	Централизованная сертификация программных продуктов в государственных органах является для корпорации Microsoft.	ПК-4

	продуктов в государственных органах для корпорации Microsoft является важным шагом к обеспечению соответствия стандартам безопасности и защиты данных. Этот процесс помогает правительственным учреждениям доверять и эффективно использовать решения Microsoft, гарантируя, что они соответствуют необходимым требованиям и нормативам. Таким образом, сертификация способствует укреплению сотрудничества между Microsoft и государственными структурами.		
56.	Органы исполнительной власти в сфере информационной безопасности работают в нескольких ключевых направлениях: разработка и внедрение национальных стандартов и нормативов, мониторинг и анализ угроз кибербезопасности, а также	Направления работы органов исполнительной власти в сфере информационной безопасности.	ПК-4

	обеспечение защиты критической информационной инфраструктуры. Также они занимаются обучением и повышением квалификации кадров, а также координацией действий с другими государственными и частными организациями для эффективного реагирования на инциденты. Эти меры направлены на создание безопасной информационной среды для граждан и организаций.		
57.	Общая политика России в сфере информационной безопасности направлена на защиту национальных интересов, информации и критической инфраструктуры от внешних и внутренних угроз. Она включает в себя разработку стратегий и нормативных актов, а также активное сотрудничество с другими государствами и международными организациями для	Общая политика России в сфере информационной безопасности.	ПК-4

	противодействия киберугрозам. Основное внимание уделяется укреплению киберзащиты и развитию технологий для обеспечения безопасности информации.		
58.	Национальная политика информационной безопасности России включает в себя доктрину, национальный план и стратегию, которые определяют основные цели и задачи в этой области. Эти документы акцентируют внимание на защите информации, критической инфраструктуры и национальных интересов, а также на развитии киберзащиты и сотрудничестве с другими странами. Важным аспектом является создание безопасной информационной среды для граждан и организаций на территории страны.	Национальная политика (доктрина, национальный план, национальная стратегия) информационной безопасности.	ПК-4
59.	Структура органов государственной власти,	Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.	ПК-4

	обеспечивающих информационную безопасность в России, включает в себя несколько ключевых ведомств, таких как Федеральная служба безопасности (ФСБ), Министерство обороны и Министерство цифрового развития. Эти органы координируют усилия по защите информации и критической инфраструктуры, разрабатывают и реализуют меры по противодействию киберугрозам. Также важную роль играют специальные комиссии и рабочие группы, занимающиеся вопросами информационной безопасности на уровне правительства.		
60.	c)	Основными рисками информационной безопасности являются: a) искажение, уменьшение объема, перекодировка информации b) техническое вмешательство, выведение из строя оборудования сети c) потеря, искажение, утечка информации d) навязанное шифрование информации с сокрытием ключа	ПК-4
61.	a)	К основным функциям системы безопасности можно отнести все перечисленное:	ПК-4

		a) установление регламента, аудит системы, выявление рисков b) установка новых офисных приложений, смена хостинг компании c) внедрение аутентификации, проверки контактных данных пользователей d) шифрование информации	
62.	a)	Принципом политики информационной безопасности является принцип … a) невозможности миновать защитные средства сети (системы) b) усиления основного звена сети, системы c) полного блокирования доступа при риск-ситуациях d) внедрение аутентификации, проверки контактных данных пользователей	ПК-4
63.	a)	Что понимается под конфиденциальностью информации? a) известность ее содержания только имеющим соответствующие полномочия субъектам b) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения c) способность обеспечения беспрепятственного доступа субъектов к интересующей их информации d) способность обеспечения беспрепятственного раскрытия смысла передаваемой информации с помощью ключа	ПК-4
64.	a)	Что понимается под целостностью информации? a) известность ее содержания только имеющим соответствующие полномочия субъектам b) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения c) способность обеспечения беспрепятственного доступа субъектов к интересующей их информации d) способность обеспечения беспрепятственного раскрытия смысла передаваемой информации с помощью ключа	ПК-4
65.	c)	Что понимается под доступностью информации?	ПК-4

		a) известность ее содержания только имеющим соответствующие полномочия субъектам b) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения c) способность обеспечения беспрепятственного доступа субъектов к интересующей их информации d) способность обеспечения беспрепятственного раскрытия смысла передаваемой информации с помощью ключа	
66.	c)	Что понимается под угрозой безопасности информации? a) возникновение явления или события в форме хищения ключа шифрования данных телекоммуникационной системы b) возникновение явления или события в форме хищения ключа шифрования ключей телекоммуникационной системы c) возникновение такого явления или события, следствием которого могут быть негативные воздействия на информацию: нарушение физической целостности, нарушение логической структуры, несанкционированная модификация, несанкционированное получение, несанкционированное размножение d) действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной её уязвимости	ПК-4
67.	a)	Что называется основными техническими средствами и системами (ОТСС)? a) это технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации, средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки и передачи конфиденциальной информации b) это технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации	ПК-4

		c) это средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки и передачи конфиденциальной информации d) это технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации	
68.	d)	Что называется вспомогательными техническими средствами и системами (ВТСС)? a) это технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации b) это средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки и передачи конфиденциальной информации c) это технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации d) это технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях	ПК-4
69.	a)	Что называется контролируемой зоной? a) это территория (либо здание, группа помещений, помещение), на которой исключено неконтролируемое пребывание лиц и транспортных средств, не имеющих постоянного или разового допуска b) это территория (либо здание, группа помещений, помещение), на которой исключено неконтролируемое пребывание лиц и транспортных средств, имеющих постоянный или разовый допуск на них c) это территория (либо здание, группа помещений, помещение), которая определяется руководством организации d) это территория (либо здание, группа помещений, помещение), которая определяется исходя из конкретной обстановки в месте расположения объекта и возможностей использования технических средств перехвата	ПК-4

70.	c)	Сколько условных уровней используется для реализации политики безопасности предприятия: a) один b) два c) три d) четыре	ПК-4
71.	a)	Как называется стандарт ГОСТ Р ИСО/МЭК 27001-2006, используемый для создания системы управления информационной безопасностью предприятия? a) Системы обеспечения информационной безопасности b) Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. c) Информационная технология. Практические правила управления информационной безопасностью. d) Информационная технология. Методы и средства обеспечения безопасности	ПК-4
72.	a)	Перечислите знания и навыки, которыми должен обладать аудитор системы менеджмента информационной безопасности предприятия. a) существующие угрозы информационной безопасности, уязвимости, меры и средства контроля и управления; организационные, правовые и договорные аспекты системы менеджмента информационной безопасности; общие знания информационной технологии и методов обеспечения информационной безопасности; методы менеджмента информационной безопасности. b) существующие угрозы информационной безопасности, уязвимости, меры и средства контроля и управления; организационные, правовые и договорные аспекты системы менеджмента информационной безопасности. c) общие знания информационной технологии и методов обеспечения информационной безопасности; методы менеджмента информационной безопасности. d) методы поиска угроз информационной безопасности. e) существующие угрозы информационной безопасности, уязвимости, меры и средства контроля и управления; организационные, правовые и договорные аспекты системы менеджмента информационной безопасности; общие знания информационной	ПК-4

		технологии и методов обеспечения информационной безопасности; методы менеджмента информационной безопасности; общие знания бизнес процессов предприятия.	
73.	d)	Что входит в перечень ценных активов компании с точки зрения информационной безопасности? a) информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.). b) сервисы (поддерживающая инфраструктура); сотрудники компании, их квалификация и опыт; нематериальные ресурсы (репутация и имидж компании). c) программное обеспечение; материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.). d) информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно исследовательская информация, документация, обучающие материалы и пр.); сервисы (поддерживающая инфраструктура); сотрудники компании, их квалификация и опыт; нематериальные ресурсы (репутация и имидж компании); программное обеспечение; материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.). e) информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.); сервисы (поддерживающая инфраструктура); сотрудники компании, их квалификация и опыт; нематериальные ресурсы (репутация и имидж компании); программное обеспечение; материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.); уставной капитал компании.	ПК-4
74.	a)	Что входит в понятие «Управление информационной безопасностью организации»? (выберите несколько правильных ответов) a) это управление персоналом, рисками, ресурсами, средствами защиты и т.п.	ПК-4

		b) это неотъемлемый элемент управления предприятием, который позволяет коллективно использовать конфиденциальную информацию, обеспечивая при этом ее защиту, а также защиту вычислительных ресурсов. c) это циклический процесс, включающий: осознание степени необходимости защиты информации; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля; распределение ролей и ответственности; обучение и мотивацию персонала; оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия. d) это процесс оценки эффективности защиты информации в организации.	
76.	a)	Влияет ли на повышение доходности бизнеса компании в целом процедура ее сертификации на соответствие международным стандартам по информационной безопасности? a) да. b) нет. c) да, при условии высокой доходности бизнеса. d) да, при условии низкой доходности бизнеса.	ПК-4
77.	b)	Что понимается под документом, определяющим перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в информационной системе (ИС), которые должны учитываться в процессе организации защиты информации, проектировании и разработке систем защиты информации, проведении проверок (контроля) защищенности ИС? a) характеристика основных (актуальных) угроз безопасности ИС. b) модель угроз безопасности ИС. c) характеристика уязвимостей ИС. d) модель уязвимостей ИС.	ПК-4

78.	a) b) c)	По каким основным причинам необходима стандартизация в области информационной безопасности(ИБ)? (выберите несколько правильных ответов) по причине имеющихся общих тенденций к стандартизации в различных сферах. a) по причине необходимости выработки единых требований по ИБ. b) по причине необходимости выработки единых подходов к решению проблем ИБ. c) по причине необходимости выработки единых качественных показателей для оценки безопасности информационной системы и средств защиты. d) по всем названным причинам.	ПК-4
79.	a) b)	Какие существуют основные группы международных стандартов в области информационной безопасности (ИБ)? (выберите несколько правильных ответов) a) группа оценочных стандартов по ИБ. b) группа, включающая в себя так называемые спецификации, регламентирующие вопросы реализации и использования методов и средств защиты информации. c) группа стандартов, объединенная в так называемую «Оранжевую книгу». d) все названные группы.	ПК-4
80.	c)	Приведите классы (подклассы) защищённости информационных систем в соответствии с «Оранжевой книгой» по мере роста защищённости информационной системы. a) Класс A — содержит единственный подкласс A1. Класс B — содержит подклассы B1, B2 и B3. Класс C — содержит подклассы C1 и C2. Класс D — содержит подкласс D1. b) Класс A — содержит единственный подкласс A1. Класс B — содержит подклассы B1 и B2. Класс C — содержит подклассы C1 и C2. Класс D — содержит подкласс D1.	ПК-4

		c) Класс D — содержит подкласс D1. Класс C — содержит подклассы C1 и C2. Класс B — содержит подклассы B1, B2 и B3. Класс A — содержит единственный подкласс A1. d) Класс D — содержит подкласс D1. Класс C — содержит подклассы C1 и C2. Класс B — содержит подклассы B1 и B2. Класс A — содержит единственный подкласс A1	
81.	b)	Какой из перечисленных стандартов служит основой при оценке характеристик безопасности ИТ-продуктов или систем для их применения с заданным уровнем риска? a) Стандарт ISO/IEC 17799 «Практические правила управления информационной безопасностью». b) Стандарт ISO/IEC 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (т.н. «Общие критерии»). c) Стандарт ISO 27001 «Информационные технологии - Методы защиты - Системы менеджмента информационной безопасности – Требования».	ПК-4

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала, оптимально расположенных на всем временном интервале изучения дисциплины.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если он, осуществляет рациональный выбор по методам защиты прав на интеллектуальную собственность, осуществляет патентные исследования в области вычислительной техники и систем связи.

Оценка «хорошо» выставляется студенту, если он, с ошибками осуществляет рациональный выбор по методам защиты прав на интеллектуальную собственность, с ошибками осуществляет патентные исследования в области вычислительной техники и систем связи.

Оценка «удовлетворительно» выставляется студенту, если он, с трудом осуществляет рациональный выбор по методам защиты прав на интеллектуальную собственность, с трудом осуществляет патентные исследования в области вычислительной техники и систем связи.

Оценка «неудовлетворительно» выставляется студенту, если он, не осуществляет рациональный выбор по методам защиты прав на интеллектуальную собственность, не осуществляет патентные исследования в области вычислительной техники и систем связи.