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
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Аудит информационных технологий и систем обеспечения информационной безопасности
название дисциплины (модуля)

Направление подготовки	10.03.01 «Информационная безопасность»
Направленность (профиль)	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	5

Введение

1. Назначение. Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Аудит информационных технологий и систем обеспечения информационной безопасности» студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

2. ФОС является приложением к программе дисциплины (модуля) «Аудит информационных технологий и систем обеспечения информационной безопасности» в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

3. Разработчик (и) Орел Д.В., доцент кафедры

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены комиссии: Жук А.П., профессор кафедры
Минкина Т.В., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «Инфоком-С»

Экспертное заключение: Фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Аудит информационных технологий и систем обеспечения информационной безопасности».

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 компетенции(й),			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ПК-3 Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации				
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-3 Способен проводить аудит защищённости информации в автоматизированных системах*	- затрудняется анализировать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - затрудняется применять инструментальные средства контроля защищённости информации в автоматизированных системах; - не проводит экспертизу состояния защищённости информации автоматизированных систем	- с большими недочетами анализирует руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - применяет основные инструментальные средства контроля защищённости информации в автоматизированных системах; - с большими недочетами проводит экспертизу состояния защищённости информации автоматизированных систем	- с незначительными замечаниями анализирует руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - с незначительными замечаниями применяет инструментальные средства контроля защищённости информации в автоматизированных системах; - с незначител	- анализирует руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; -применяет инструментальные средства контроля защищённости информации в автоматизированных системах; -проводит экспертизу состояния защищённости информации автоматизированных систем

			ьными замечаниям и проводит экспертизу состояния защищённо сти информаци и автоматизи рованных систем	
Компетенция: ПК-6 Способен проводить контроль защищённости информации				
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-2 Способен проводить контроль защищённости информации от несанкционирова нного доступа*	- затрудняется проводить оценку защищенности информации от несанкционированно го доступа и специальных воздействий; - затрудняется оформлять отчетные материалы по результатам контроля защищенности информации от несанкционированно го доступа и специальных воздействий (протокол контроля защищенности информации от несанкционированно го доступа и специальных воздействий).	- в целом проводит оценку защищенности информации от несанкционирова нного доступа и специальных воздействий; - со значительными замечаниями оформляет отчетные материалы по результатам контроля защищенности информации от несанкционирова нного доступа и специальных воздействий (протокол контроля защищенности информации от несанкционирова нного доступа и специальных воздействий).	- с незначител ьными замечаниям и проводит оценку защищенно сти информаци и от несанкцион ированного доступа и специальны х воздействи й; - с незначител ьными замечаниям и оформляет отчетные материалы по результата м контроля защищенно сти информаци и от несанкцион ированного доступа и специальны х воздействи й (протокол контроля	- проводит оценку защищенно сти информаци и от несанкцио нированног о доступа и специальн ых воздействи й; - оформляет отчетные материалы по результата м контроля защищенно сти информаци и от несанкцио нированног о доступа и специальн ых воздействи й (протокол контроля защищенно сти информаци и от несанкцио нированног о доступа и

			защищенности информации от несанкционированного доступа и специальных воздействий).	специальных воздействий).

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 ОФО семестр 5,	
1.	A, b, c, d	Что входит в понятие главной цели системы обеспечения ИБ? a) создание условий функционирования предприятия b) предотвращение угроз безопасности предприятия c) защита законных интересов предприятия от противоправных посягательств d) недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации e) Ничего не подходит	ПК-6
2.	A, b, c, d	Назовите основные задачи системы ИБ. a) необходимость отнесения определенной информации к категории ограниченного доступа (служебной или коммерческой тайне) b) прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития c) создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба d) создание механизма и условий оперативного реагирования на угрозы ИБ и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности e) создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения ИБ f) Ничего не подходит	ПК-6
3.	B, d, e	Какие виды угроз ИБ встречаются наиболее часто?	ПК-6

		a) хищение – совершенные с корыстной целью противоправное безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или владельцу имущества b) копирование компьютерной информации – повторение и устойчивое запечатление информации на машинном или ином носителе c) уничтожение – внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводится в полную непригодность для использования по целевому назначению d) уничтожение компьютерной информации – стирание ее в памяти ЭВМ e) повреждение – изменение свойств имущества, при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования f) модификация компьютерной информации – внесение любых изменений, связанных с адаптацией программы для ЭВМ или баз данных g) блокирование компьютерной информации – искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением h) несанкционированное уничтожение, блокирование, модификация, копирование информации – любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией i) обман (отрицание подлинности, навязывание ложной информации) – умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество, и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью ложных сведений.	
4.	A, c	Приведите примеры источников угроз. a) неквалифицированная корпоративная политика по организации информационных технологий и управлению безопасностью корпорации; b) отсутствие должной квалификации персонала по обеспечению деятельности и управлению объектом защиты;	ПК-6

		c) преднамеренные и непреднамеренные действия персонала по нарушению безопасности; d) техногенные аварии и разрушения, пожары.	
5.	a-e	Основные модули модели реализации угроз ИБ. a) угроза b) источник угрозы c) метод реализации d) уязвимость e) последствия	ПК-6
6.		Какие существуют методы парирования угроз? a) экономические b) организационные c) инженерно-технические d) технические e) программно-аппаратные	ПК-6
7.		Назвать основные компоненты модели построения системы ИБ. a) Владелец информации b) Контрмеры c) Уязвимости d) Риск e) Угрозы f) Ресурс	ПК-6
8.		С какой целью разрабатывается концепция ИБ? a) Современный подход к обеспечению безопасности требует создания целостной системы ИБ, включающей в себя комплекс организационных, правовых, инженерно-технических и программно-аппаратных мер защиты, использующей современные методы прогнозирования, анализа и моделирования постоянно изменяющихся ситуаций b) На основе анализа современного достигнутого уровня и динамики развития информационных технологий, ожидаемых угроз ИБ, источников этих угроз и факторов, способствующих их реализации, дается систематизированное	ПК-6

		изложение целей, задач и принципов достижения требуемого уровня информационной безопасности	
9.		Из каких разделов состоит концепция ИБ? a) Правовое обеспечение вопросов защиты информации. b) Цели и задачи защиты информации. c) Информация, подлежащая защите. d) Техническая политика и принципы построения защиты. e) Модель угроз информационной безопасности.	ПК-6
10.		В чем отличие и особенности проведения внешнего и внутреннего аудита? a) Внешний аудит – это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Рекомендуется проводить внешний аудит регулярно, а, например, для многих финансовых организаций и акционерных обществ это является обязательным требованием со стороны их учредителей и акционеров. b) Внутренний аудит представляет собой непрерывную деятельность, которая осуществляется на основании «Положения о внутреннем аудите» и в соответствии с планом, подготовка которого осуществляется подразделениями службы безопасноти и утверждается руководством организации.	ПК-3
11.		Назовите основные цели проведения аудита ИБ. a) анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов b) оценка текущего уровня защищенности ИС c) локализация узких мест в системе защиты ИС d) оценка соответствия ИС существующим стандартам в области информационной безопасности e) выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.	ПК-3
12.		Какая последовательность действий при проведении аудита ИБ на предприятии? a) Подготовка к проведению аудита безопасности b) Проведение аудита	ПК-3

		c) Завершение аудита	
13.		Чем определяются масштабы аудита ИБ? a) аудит безопасности всего предприятия в комплексе b) аудит безопасности отдельных зданий и помещений (выделенные помещения) c) аудит оборудования и технических средств конкретных типов и видов d) аудит отдельных видов и направлений деятельности: экономической, экологической, информационной, финансовой и т. д.	ПК-3
14.		С какой целью проводится анализ рисков? a) Включает в себя мероприятия по обследованию безопасности предприятия с целью определения того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите b) Определение набора адекватных контрмер осуществляется в ходе управления рисками. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого ресурсам информационных систем (ИС), в случае осуществления угрозы безопасности выявить существующие риски и c) Оценить их величину (дать им качественную, либо количественную оценку)	ПК-3
15.		Назовите задачи, решаемые при анализе рисков. a) Идентификация ключевых ресурсов ИС b) Определение важности тех или иных ресурсов для организации c) Идентификация существующих угроз безопасности и уязвимостей, делающих возможным осуществление угроз. d) Вычисление рисков, связанных с осуществлением угроз безопасности.	ПК-3
16.		Как может быть оценена величина риска? a) на основе стоимости ресурса b) на основе вероятности осуществления угрозы c) на основе величины уязвимости	ПК-3
17.		Какие этапы включает сценарий анализа информационных ресурсов? a) определяются сведения, которые составляют для предприятия коммерческую тайну и которые предстоит защищать	ПК-3

		b) построение каналов доступа, утечки или воздействия на информационные ресурсы основных узлов ИС c) анализ способов защиты всех возможных точек атак соответствует целям защиты и его результатом должна быть характеристика возможных брешей в обороне, в том числе за счет неблагоприятного стечения обстоятельств d) определяются вероятности реализации угроз по каждой из возможных точек атак e) оценивается ущерб организации в случае реализации каждой из атак, который вместе с оценками уязвимости позволяет получить ранжированный список угроз информационным ресурсам.	
18.		В чем состоит суть (подходы) управления рисками? a) системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями российской нормативно-правовой базы в области защиты информации и собственной корпоративной политики безопасности b) объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности предприятия	ПК-6
19.		По каким показателям проводится оценивание информационных рисков? a) безопасность персонала b) разглашение частной информации c) требования по соблюдению законодательных и нормативных положений d) ограничения, вытекающие из законодательства e) коммерческие и экономические интересы f) финансовые потери и нарушения в производственной деятельности; g) общественные отношения h) коммерческую политику и коммерческие операции i) потерю репутации компании	ПК-6
20.		Содержание алгоритма оценивания рисков. a) описание объекта и мер защиты	ПК-6

		b) идентификация ресурса и оценивание его количественных показателей (определение потенциального негативного воздействия на бизнес) c) анализ угроз информационной безопасности d) оценивание уязвимостей e) оценивание существующих и предполагаемых средств обеспечения информационной безопасности f) оценивание рисков	
21.		Назовите этапы процесса управления рисками. a) Выбор анализируемых объектов и уровня детализации их рассмотрения. b) Выбор методологии оценки рисков. c) Идентификация активов. d) Анализ угроз и их последствий, выявление уязвимых мест в защите. e) Оценка рисков. f) Выбор защитных мер. g) Реализация и проверка выбранных мер. h) Оценка остаточного риска.	ПК-3
22.		С какой целью разрабатывались международные стандарты ИБ? строго определяются цели обеспечения информационной безопасности компьютерных систем a) создается эффективная система управления информационной безопасностью b) обеспечивается расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям c) создаются условия применения имеющегося инструментария (программных средств) обеспечения информационной безопасности и оценки ее текущего состояния d) открывается возможность использования методик управления безопасностью с обоснованной системой метрик и мер обеспечения разработчиков информационных систем	ПК-6
23.		Назовите основные международные стандарты ИБ.	ПК-3

		a) Критерий оценки надежности компьютерных систем «Оранжевая книга» (США); b) Гармонизированные критерии европейских стран; c) Рекомендации X.800; d) Германский стандарт BSI; e) Британский стандарт BS 7799; f) Стандарт ISO 17799; g) Стандарт «Общие критерии» ISO 15408; h) Стандарт COBIT	
24.		Какие критерии определяют степень доверия в стандарте «Оранжевая книга»? a) Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию b) Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС	ПК-3
25.		Определите назначения и виды классов безопасности в «Оранжевой книге». a) В "Оранжевой книге" рассматривается четыре уровня безопасности (надежности) — D, C, B и A. b) D1 – неудовлетворительная безопасность; c) C1, C2 – произвольное управление доступом; d) B1, B2, B3 – принудительное управление доступом; e) A1 – верифицированная защита.	ПК-3
26.		Как определяются составляющие ИБ в гармозированных критериях Европейских стран. a) конфиденциальность, то есть защиту от несанкционированного получения информации b) целостность, то есть защиту от несанкционированного изменения информации c) доступность, то есть защиту от несанкционированного удержания информации и ресурсов	ПК-3
27.		Приведите составляющие германского стандарта BSI.	ПК-3

		a) Общий метод управления информационной безопасностью (организация менеджмента в области ИБ, методология использования руководства) b) Основные компоненты (организационный уровень ИБ, процедурный уровень, организация защиты данных, планирование действий в чрезвычайных ситуациях) c) Инфраструктура (здания, помещения, кабельные сети, организация удаленного доступа) d) Клиентские компоненты различных типов (DOS, Windows, UNIX, мобильные компоненты, прочие типы) e) Сети различных типов (соединения «точка-точка», сети Novell NetWare, сети с ОС ONIX и Windows, разнородные сети) f) Элементы систем передачи данных (электронная почта, модемы, межсетевые экраны и т.д.).	
28.		Почему Британский стандарт BS 7799 используется наиболее часто? a) Был принят в качестве национального стандарта управления информационной безопасностью организации вне зависимости от сферы деятельности компании b) В соответствии с этим стандартом любая служба безопасности, IT -отдел, руководство компании должны начинать работать согласно общему регламенту	ПК-3
29.		В чем отличие применения международных стандартов ISO 15408 и ISO 17799? a) В определенном смысле роль функциональных стандартов выполняют профили защиты, которые формируются с учетом рекомендаций и каталога требований ОК, но могут включать и любые другие требования, которые необходимы для обеспечения безопасности конкретного изделия или типа изделий ИТ b) По уровню систематизации, полноте и возможностям детализации требований, универсальности и гибкости в применении ОК представляют наиболее совершенный из существующих в настоящее время стандартов c) В силу особенностей построения стандарт ISO 15408 имеет практически неограниченные возможности для развития, представляет собой не	ПК-3

		функциональный стандарт, а методологию задания, оценки и каталог требований безопасности ИТ, который может наращиваться и уточняться	
30.		Назовите основные этапы проведения аудита ИБ при использовании стандарта CoBiT. a) Подписание договорной и исходно-разрешительной документации b) Сбор информации c) Анализ исходных данных d) Выработка рекомендаций e) Контроль за выполнением рекомендаций f) Подписание отчетных актов g) Планирование и организация работы h) Приобретение и ввод в действие i) Поставка и поддержка j) Мониторинг	ПК-3
31.		Какие стандарты, разработанные в России, используются при оценке защищенности информационных технологий? a) ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. архитектура защиты информации. b) ГОСТ Р ИСО/МЭК 9594-8-98 Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. основы аутентификации c) ГОСТ Р ИСО/МЭК 9594-9-95 Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 9. Дублирование d) ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».	ПК-3
32.		Опишите статус стандарта ISO 15408 в РФ. a) «Общие критерии» неоднократно редактировались. В результате 8 июня 1999 года был утвержден Международный стандарт ISO/IEC 15408 под названием «Общие критерии оценки безопасности информационных технологий» (ОК)	ПК-3

		b) Общие критерии обобщили содержание и опыт использования «Оранжевой книги», развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США	
33.		Что включает в себя понятие «доверие» в рамках стандарта ISO15408? a) основа для уверенности в том, что продукт или система отвечают целям и требованиям безопасности b) оценка процесса функционирования системы для определения его свойств безопасности	ПК-3
34.		Какие классы и семейства используются для оценки безопасности ПС? a) Класс управление конфигурацией ПС b) Класс поставка и эксплуатация ПС c) Класс разработка ПС d) Класс руководства по безопасности ПС e) Класс поддержка жизненного цикла ПС	ПК-3
35.		Дайте определение понятиям «профиль защиты» и «Задание по безопасности». a) Профиль защиты (ПЗ) – независимая от реализации совокупность требований безопасности для некоторой категории объектов, отвечающая специфическим требованиям проекта и потребителя. b) Задание по безопасности (ЗБ) – совокупность требований и спецификаций, предназначенная для использования в качестве основы для оценки конкретного объекта.	ПК-3
36.		Что определяет оценочный уровень доверия (ОУД)? a) В зависимости от сложности и критичности требования к безопасности функционирования системы и доступных ресурсов для ее реализации, стандартом рекомендуется выбирать набор классов и семейств процессов, достаточных для обеспечения необходимого качества комплекса функциональной безопасности проекта b) Образуют возрастающую шкалу достигаемого качества безопасности, которая позволяет соотнести получаемый уровень качества с трудоемкостью его реализации и возможностью достижения этой степени доверия	ПК-3

37.		Изложите общую схему оценки безопасности ИТ на основе общих критериев. a) ОК поддерживают выбор и оценку безопасности объекта ИТ. ОК полезны при разработке изделий или систем ИТ с функциями безопасности и при приобретении коммерческих изделий и систем с такими функциями. ОК дают основу для оценки объекта, чтобы установить уровень доверия к безопасности ИТ. b) Аспекты безопасности ИТ включают защиту информации от несанкционированного раскрытия, модификации или потери возможности использования при воздействии угроз, являющихся результатом преднамеренных или непреднамеренных действий человека. Защищенность от этих трех типов угроз обычно называют конфиденциальностью, целостностью и доступностью.	ПК-3
38.		Назовите 10 разделов для управления ИБ по стандарту ISO 17799. a) Политика безопасности b) Организационные меры по обеспечению безопасности c) Классификация ресурсов и их контроль d) Безопасность персонала e) Физическая безопасность f) Администрирование компьютерных систем и вычислительных сетей g) Управление доступом к системам h) Разработка и сопровождение информационных систем i) Планирование бесперебойной работы организации j) Соответствие системы основным требованиям	ПК-3
39.		Расскажите о ключевых средствах контроля ИБ предприятия. a) Документ о политике информационной безопасности b) Распределение обязанностей по обеспечению информационной безопасности. c) Обучение и подготовка персонала к поддержанию режима информационной безопасности d) Уведомление о случаях нарушения защиты e) Средства защиты от вирусов	ПК-3

40.		Дайте определения понятия «Политика безопасности» и опишите особенности его разработки. a) Политика безопасности в целом – это совокупность программных, аппаратных, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, четко регламентирующих все аспекты деятельности компании, включая информационную систему, и обеспечивающих их безопасность b) Политика безопасности является одним из важнейших, жизненно важных документов компании c) Необходимость разработанной соответствующей политики безопасности на сегодняшний день является очевидным фактом для любой, даже достаточно небольшой компании	ПК-3
41.		Опишите основные положения политики обеспечения информационной безопасности. a) Определение информационной безопасности, перечень ее составляющих. b) Положение о целях управления - поддержка целей и принципов информационной безопасности c) Краткое разъяснение политики безопасности, принципов ее построения и стандартов в этой области d) Включение в должностные обязанности руководителей ответственности за обеспечение информационной безопасности, включая отчеты об инцидентах e) Подробный перечень документов, которые должны быть изданы вместе с политикой безопасности (положения, инструкции, регламенты и т.п.)	ПК-3
42.		Какие организационные меры используются при управлении ИБ? a) Координация действий по защите информации b) Независимый анализ информационной безопасности	ПК-3
43.		Назовите вопросы, которые рассматриваются при заключении контрактов со сторонними организациями. a) общая политика информационной безопасности; разрешенные способы доступа, а также контроль и использование уникальных идентификаторов пользователей и паролей	ПК-3

		b) описание каждого предоставляемого информационного сервиса c) требование вести список лиц, которым разрешено использовать сервис d) время и дата, когда сервис будет доступен e) процедуры, касающиеся защиты ресурсов организации, включая информацию	
44.		Приведите классификацию ресурсов и опишите уровни их защиты. a) информационные ресурсы: базы данных и файлы данных, системная документация, руководства пользователя, учебные материалы, операционные процедуры и процедуры поддержки, планы обеспечения бесперебойной работы организации, процедуры перехода на аварийный режим b) программные ресурсы: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты c) физические ресурсы: компьютеры и коммуникационное оборудование, магнитные носители данных (ленты и диски), другое техническое оборудование (блоки питания, кондиционеры), мебель, помещения d) сервисы: вычислительные и коммуникационные сервисы, другие технические сервисы (отопление, освещение, энергоснабжение, кондиционирование воздуха).	ПК-3
45.		Перечислите правила безопасности при выборе и работе с персоналом. a) Безопасность в должностных инструкциях b) Проверка принимаемых на работу c) Соглашение о конфиденциальности d) Условия работы персонала	ПК-3
46.		Какие вопросы должны рассматриваться при обучении персонала? a) Реагирование на события, таящие угрозу безопасности b) Уведомление об инцидентах в системе безопасности c) Уведомление о слабых местах в системе безопасности d) Уведомление об отказах программного обеспечения e) Процедура наложения дисциплинарных взысканий	ПК-3

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется, если студент показал глубокое, прочное и аргументированное освоение программного учебного материала, при этом поставленный вопрос раскрыт последовательно, четко и логически стройно, в полном исчерпывающем объеме, основные категории, понятия и термины учебного курса формулировались правильно, не допущено при ответе ошибок

Оценка «хорошо» выставляется, если студент показал твердое знание программного учебного материала, при этом поставленный вопрос раскрыт грамотно и по существу, в достаточно полном объеме, основные категории, понятия и термины учебного курса формулировались правильно, допущены при ответе отдельные неточности или одна ошибка;

Оценка «удовлетворительно» выставляется, если студент показал знание только основной части учебного материала без его частных деталей, при этом поставленный вопрос раскрыт с нарушением логической последовательности, не в полном объеме, были допущены неточные формулировки основных категорий, понятий и терминов учебного курса, а также ошибки (не более двух) или ряд незначительных неточностей, не исказивших существенно суть ответа;

Оценка «неудовлетворительно» выставляется, студенту, который не знает значительной части программного материала, допускает грубые ошибки (более двух), существенно исказившие его суть. Оценка неудовлетворительно выставляется также, если отсутствует письменный ответ на вопрос, либо студент отказался его сдавать.

**** в соответствии с результатами освоения дисциплины и видами заданий***