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
ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ
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	7

Введение

1. Назначение: оценить уровень сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации по дисциплине «Защита информации в системах беспроводной связи» студентов, обучающихся по направлению подготовки 10.03.01 Информационная безопасность (профиль «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»).

2. Фонд оценочных средств текущего контроля успеваемости и промежуточной аттестации разработан на основе рабочей программы дисциплины «Защита информации в системах беспроводной связи» и в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 Информационная безопасность (профиль «Организация и технология защиты информации (по отрасли или в сфере профессиональной деятельности).

3. Разработчик: А.П. Жук профессор кафедры организации и технологии защиты информации

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель: В.И. Петренко, зав. кафедрой организации и технологии защиты информации

Члены экспертной группы:

В.Е. Рачков, к.т.н., доцент кафедры организации и технологии защиты информации.

В.М. Бисюков, доцент кафедры организации и технологии защиты информации.

Орел Д.В., к.т.н., доцент кафедры организации и технологии защиты информации.

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 «Защита информации в системах беспроводной связи».

5. Срок действия ФОС: на срок 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-1 Способен обеспечивать защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи (за исключением сетей связи специального назначения) в процессе их эксплуатации				
Результаты обучения по дисциплине (модулю): *Индикатор:* Способен проводить мониторинг функционирования СССЭ, защищённости от НСД сооружений и СССЭ	Не определяет - необходимые способы мониторинга функционирования беспроводных СССЭ и не оценивает базовые показатели их защищенности от НСД к информации	Не определяет минимально-необходимые способы мониторинга функционирования беспроводных СССЭ и не оценивает базовые показатели их защищенности от НСД к информации	Определяет минимально-необходимые способы мониторинга функционирования беспроводных СССЭ и оценивает базовые показатели их защищенности от НСД к информации	Определяет основные способы мониторинга функционирования беспроводных СССЭ и оценивает основные показатели их защищенности от НСД к информации

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.

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения ОФО семестр 1	
	а)	**Вопрос №1.** Какой вариант в полном объеме характеризует понятие угрозы безопасности информации? a) ***понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств***. b) потенциально возможное событие, процесс или явление, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам. c) возможность реализации воздействия на информацию, обрабатываемую в АИС, приводящего к нарушению конфиденциальности, целостности или доступности этой информации, а также возможность воздействия на компоненты АИС, приводящего к их утрате, уничтожению или сбою функционирования. d) потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.	ПК-1
	а)	**Вопрос №2.** Потенциальные угрозы, против которых направлены технические меры защиты информации ***а) Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей*** b) Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения c) Потери информации из-за не достаточной установки резервных систем электропитании	ПК-1

		и оснащение помещений замками. d) Потери информации из-за не достаточной установки сигнализации в помещении. e) Процессы преобразования, при котором информация удаляется	
	a)	**Вопрос №3.** Оценка рисков позволяет ответить на следующие вопросы: a) ***чем рискует организация, используя информационную систему?*** b) чем рискуют пользователи информационной системы? c) чем рискуют системные администраторы?	ПК-1
	a)	**Вопрос №4.** Целью проведения аудита информационной безопасности является ***a) оценка состояния информационной безопасности организации, ее информационной системы, и разработка рекомендаций по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных и иных ресурсов*** b) оценка состояния информационной c) безопасности организации, ее информационной системы, и разработка рекомендаций по проектированию комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных и иных ресурсов.	ПК-1
	a) b) c)	**Вопрос №5.** Из приведенного ниже списка выделите виды аудита информационной безопасности **a)** ***активный аудит (внутренний и внешний)*****;** b) ***экспертный аудит***; c) ***аудит на соответствие стандартам информационной безопасности***; d) финансовый аудит;	ПК-1

		e) аудит на соответствие стандартам менеджмента и качества**.**	
	a) b) c) d)	**Вопрос №7.** Процесс анализа рисков предусматривает решение следующих задач ***a) идентификация ключевых ресурсов информационной системы;*** ***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;*** e) аутентификация пользователей информационной системы; f) верификация пользователей локально-вычислительной сети; g) идентификация пользователей информационной системы.	ПК-1
	e)	**Вопрос №8.** К основным целям криптографии относятся: a) Обеспечение конфиденциальности; b) Обеспечение целостности; c) Обеспечение аутентификации; d) Обеспечение невозможности отказа от авторства; **e)** ***Всё выше перечисленное.***	ПК-1
	a)	**Вопрос №9.** Как называется преобразовательный процесс, в котором исходный текст заменяется шифрованным текстом? **a)** ***Шифрование (зашифрование)*****;**	ПК-1

		b) Кодирование; c) Дешифрование; d) Расшифрование; e) Криптование.	
	a)	**Вопрос №10.** Разработка и внедрение новых информационно-вычислительных систем, в рамках которых решается весь комплекс проблем защиты информации это **a) *креативный подход*;** b) аддитивный подход; c) интеграционный подход.	ПК-1
	a) b) f) g)	**Вопрос №1.** Из приведенного ниже списка выделите задачи мониторинга **a) *прогнозирование;*** **b) *разработка приемов и способов приведения объекта мониторинга в оптимальное состояние;*** c) проектирование; d) аудит информационной безопасности; e) сбор фактического материала, результатом которого является получение определенной информации о данном объекте; ***f) оценивание;*** **g) *контроль.***	ПК-1
	a)	**Вопрос №3.** Какие вирусы активизируются в самом начале работы с операционной	ПК-1

		системой: **a) *загрузочные вирусы;*** b) троянцы; c) черви.	
	a)	**Вопрос №2.** Какой структурно-функциональный элемент информационной системы не может быть подвержен формальному администрированию при реализации мер защиты информации **a) *Сеть общего пользования.*** b) Рабочие станции организации. c) Сетевые устройства. d) Сервер организации	ПК-1
	b)	**Вопрос №4.** Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству: a) снизить уровень классификации этой информации; **b) *улучшить контроль за безопасностью этой информации;*** c) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации.	ПК-1
	a) b)	**Вопрос №5.** К техническим средствам и системам оповещения относятся: **a) *Инфракрасные датчики*** **b) *Электрические датчики***	ПК-1

		c) Электромеханические датчики d) Электрохимические датчики	
	a)	**Вопрос №6.** Защита от сбоев серверов, рабочих станций и локальных компьютеров относится? **a)** ***аппаратным средствам защиты;*** b) программным средствам защиты; c) техническим средствам защиты; d) правовым средствам защиты.	ПК-1
	a)	**Вопрос №1.** Технология проектирования систем радиомониторинга базируется: **a)** ***На временном или спектральном анализе принимаемых сигналов*****;** b) На возможности обнаружения и приема (регистрация) сигнала; c) На реализации обработки (анализ) принятых сигналов; d) На возможности восстановления информации, содержащейся в принятых сигналах, и ее анализе.	ПК-1
	b)	**Вопрос №2.** Укажите, что из приведенного перечня является одним из видов проектного анализа: a) ситуационный; **b)** ***организационный*****;** c) экологический; d) финансовый.	ПК-1

	a)	**Вопрос №3.** Данный способов подключения к Интернет обеспечивает наибольшие возможности для доступа к информационным ресурсам: **a)** ***Постоянное соединение по оптоволоконному каналу*** b) Удаленный доступ по коммутируемому телефонному каналу c) Постоянное соединение по выделенному телефонному каналу Терминальное соединение по коммутируемому телефонному каналу	ПК-1
	b) c) e)	**Вопрос №5.** Укажите стандартные процессы жизненного цикла информационной системы, используемые в процессе ее создания и функционирования a) Основные процессы производства. **b)** ***Основные процессы жизненного цикла.*** **c)** ***Вспомогательные процессы жизненного цикла.*** d) Вспомогательные процессы маркетинга. **e)** ***Организационные процессы жизненного цикла.*** f) Организационные циклы логистики. g) Процессы планирования. h) Процессы учета.	ПК-1
	d)	**Вопрос №6**. Укажите информационные модели, разработка которых регламентируется соглашениями, принятыми в практике создания информационных систем Варианты ответа: a) Сетевые модели. b) Иерархические модели.	ПК-1

		c) Реляционные модели. **d)** ***Диаграммы потоков данных.*** e) Графовые модели.	
	a) b) c)	**Вопрос№1.** Задача оценки эффективности КСЗИ может разбиваться на следующие частные задачи: **a)** ***Оценки эффективности защиты от сбоев и отказов аппаратных и программных средств*****;** **b)** ***Оценки эффективности защиты от НСДИ*****;** **c)** ***Оценки эффективности защиты от ПЭМИН*****;** d) Оценки способности персонала соблюдать политику информационной безопасности.	ПК-1
	c)	**Вопрос №2.** Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании? a) Чтобы убедиться, что проводится справедливая оценка. b) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ. **c)** ***Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа.*** d) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку.	ПК-1

	b) c)	**Вопрос №3.** Какие свойства информации выполняет резервное копирование? a) конфиденциальность; **b) *целостность*;** **c) *доступность*.**	ПК-1
	a)	**Вопрос №4.** Для усовершенствования собственных процессов и систем, их соответствия требованиям и определения пригодности процессов и систем одной организации для другой на договорной основе - необходим **a) *контроль и проверка процессов систем организации*;** b) контроль и проверка финансового состояния организации; c) контроль и проверка процессов систем пожарной сигнализации.	ПК-1
	a) b) c) d) e) f)	**Вопрос №5.** Какие пункты включает в себя план проведения аудита информационной безопасности ***a) цель аудита информационной безопасности;*** ***b) критерии аудита информационной безопасности и ссылочные документы;*** ***c) область аудита информационной безопасности;*** ***d) дату и продолжительность проведения аудита информационной безопасности на месте;*** ***e) роли членов аудиторской группы и сопровождающих лиц со стороны проверяемой организации;*** ***f) результаты анализа документов, предоставленных проверяемой организацией для проведения аудита информационной безопасности, и оценку свидетельств***	ПК-1

		аудита информационной безопасности; ***g) описание деятельности и мероприятий по проведению аудита информационной безопасности на месте;*** h) методика оценивания рисков информационной системы; i) методы оценки угроз и уязвимостей информационной системы; j) роли руководящего состава организации; k) методика оценки угроз.	
	a) b) c)	**Вопрос№1.** Задача оценки эффективности КСЗИ может разбиваться на следующие частные задачи: **a) *Оценки эффективности защиты от сбоев и отказов аппаратных и программных средств*;** **b) *Оценки эффективности защиты от НСДИ*;** **c) *Оценки эффективности защиты от ПЭМИН*;** d) Оценки способности персонала соблюдать политику информационной безопасности.	ПК-1
	c)	**Вопрос №2.** Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании? a) Чтобы убедиться, что проводится справедливая оценка. b) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ. **c) *Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную***	ПК-1

		информацию для анализа. d) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку.	
	b) c)	**Вопрос №3.** Какие свойства информации выполняет резервное копирование? a) конфиденциальность; **b) *целостность*;** **c) *доступность*.**	ПК-1
	a)	**Вопрос №4.** Для усовершенствования собственных процессов и систем, их соответствия требованиям и определения пригодности процессов и систем одной организации для другой на договорной основе - необходим **a) *контроль и проверка процессов систем организации*;** b) контроль и проверка финансового состояния организации; c) контроль и проверка процессов систем пожарной сигнализации.	ПК-1
	a) b) c) d) e) f)	**Вопрос №5.** Какие пункты включает в себя план проведения аудита информационной безопасности ***a) цель аудита информационной безопасности;*** ***b) критерии аудита информационной безопасности и ссылочные документы;*** ***c) область аудита информационной безопасности;*** ***d) дату и продолжительность проведения аудита информационной безопасности на месте;*** ***e) роли членов аудиторской группы и сопровождающих лиц со стороны***	ПК-1

		проверяемой организации; ***f) результаты анализа документов, предоставленных проверяемой организацией для проведения аудита информационной безопасности, и оценку свидетельств аудита информационной безопасности;*** ***g) описание деятельности и мероприятий по проведению аудита информационной безопасности на месте;*** h) методика оценивания рисков информационной системы; i) методы оценки угроз и уязвимостей информационной системы; j) роли руководящего состава организации; k) методика оценки угроз.	
	a) b) c) d) e)	**Вопрос №6.** Из приведенного ниже списка выделите методы нейтрализации угроз информационной безопасности a) ***экономические***; **b) *организационные*;** c) ***инженерно-технические***; **d) *технические*;** e) ***программно-аппаратные***; f) эргономические; g) страхование; h) математические; i) физические.	ПК-1

		Классификация беспроводных видов связи (технологии).	ПК-1
		Преимущества сетей подвижной связи (СПС).	ПК-1
		Перечислите классы сетей подвижной связи.	ПК-1
		Что понимается под термином «транкинг»?	ПК-1
		Какие существуют системы транкинговой связи?	ПК-1
		Ключевая особенность сотовой связи.	ПК-1
		Оптическая беспроводная связь, ее особенности.	ПК-1
		На какие группы делятся инфракрасные каналы связи?	ПК-1
		Наиболее распространенные способы построения беспроводных локальных сетей?	ПК-1
		Перечислить основные типы сетей беспроводного абонентского доступа.	ПК-1
		Многоканальный доступ: преимущества и недостатки.	ПК-1
		Объяснить принцип МДЧР и МДВР.	ПК-1
		Пояснить кодовое разделение каналов.	ПК-1
		Основные характеристики широкополосного сигнала.	ПК-1
		Каким образом передается сигнал в системе беспроводной оптической связи?	ПК-1
		Перечислите преимущества беспроводной оптической связи.	ПК-1
		Назовите недостатки беспроводной оптической связи.	ПК-1
		Какие проблемы существуют в сотовой связи?	ПК-1
		Предлагаемые пути решения проблем в сотовой связи.	ПК-1
		Способы организации связи между станцией и подвижным абонентом.	ПК-1
		Какие факторы влияют на определение радиуса зоны уверенного приема?	ПК-1
		Характеристика лазерных и инфракрасных систем.	ПК-1
		Какие модели потерь радиосигналов существуют?	ПК-1
		Какие показатели и характеристики информации Вы знаете?	ПК-1
		Стандарты аутентификации IEEE 802.11 сети с традиционной безопасностью.	ПК-1
		Стандарт сети 802.11i с повышенной безопасностью (WPA2)	ПК-1
		Стандарт 802.1x/EAP (Enterprise-режим) характеристика.	ПК-1
		Развертывание беспроводных виртуальных сетей	ПК-1
		Топология "хост-сеть"	ПК-1
		Топология "хост-хост"	ПК-1
		Топология "сеть-сеть"	ПК-1

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 студенту, если_____
_____

Оценка «хорошо» выставляется студенту, если_____
_____

Оценка «удовлетворительно» выставляется студенту, если_____
_____

Оценка «неудовлетворительно» выставляется студенту, если_____
_____

*Оценка «зачтено» выставляется студенту, если*_____
_____

*Оценка «не зачтено» выставляется студенту, если*_____
_____

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