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
АТТЕСТАЦИЯ ОБЪЕКТОВ 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: оценить уровень сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации по дисциплине «Аттестация объектов 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. Фонд оценочных средств текущего контроля успеваемости и промежуточной аттестации разработан на основе рабочей программы дисциплины «Аттестация объектов информационной безопасности» и в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 Информационная безопасность (профиль «Организация и технологии 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 технология 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-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	не проводит аудит защищённости информации на объектах информационной безопасности в минимально-допустимом объеме мероприятий	проводит аудит защищённости информации на объектах информационной безопасности в минимально-допустимом объеме мероприятий	проводит аудит защищённости информации на объектах информационной безопасности в объеме основных мероприятий	проводит аудит защищённости информации на объектах информационной безопасности в полном объеме
Компетенция: ПК-6 - Способен проводить контроль защищённости информации				
Результаты обучения по дисциплине (модулю): *Индикатор:* ***ИД-2*** Способен проводить контроль защищённости информации от несанкционированного доступа	Проводит оценку защищенности информации от несанкционированного доступа и специальных воздействий в недопустимом объеме Оформлять отчетные материалы по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий (протокол контроля защищенности информации от несанкционированного доступа и специальных	Проводит оценку защищенности информации от несанкционированного доступа и специальных воздействий в минимально допустимом объеме Оформляет отчетные материалы по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий (протокол контроля защищенности информации от несанкционированного доступа и	Проводит оценку защищенности информации от несанкционированного доступа и специальных воздействий в допустимом объеме Оформляет практически все отчетные материалы по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий (протокол контроля защищенности	Проводит оценку защищенности информации от несанкционированного доступа и специальных воздействий Оформляет отчетные материалы по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий (протокол контроля защищенности информации от несанкциониро

	воздействий) в недопустимом объеме	специальных воздействий) в минимально допустимом объеме	информации от несанкционированного доступа и специальных воздействий)	ванного доступа и 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.

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения ОФО семестр 1	
	c)	К правовым методам, обеспечивающим информационную безопасность, относятся: a) Разработка аппаратных средств обеспечения правовых данных; b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий; c) ***Разработка и конкретизация правовых нормативных актов обеспечения безопасности***.	ПК-6
	c)	Что понимается под понятием «Конфиденциальность персональных данных»? a) Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных; b) Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотренное федеральным законом; c) ***Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания***.	ПК-6
	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***.	ПК-6
	b)	Основными субъектами информационной безопасности являются: a) руководители, менеджеры, администраторы компаний; b) ***органы права, государства, бизнеса****;* c) сетевые базы данных, фаерволлы.	ПК-6
	c)	Наиболее важным при реализации защитных мер политики безопасности является: a) Аудит, анализ затрат на проведение защитных мер;	ПК-6

		b) Аудит, анализ безопасности; ***c) Аудит, анализ уязвимостей, риск-ситуаций***.	
	a)	Обязательной аттестации подлежат объекты информатизации, предназначенные для: a) ***Обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров***. b) Обработки информации представляющей коммерческую тайну. c) Обработки информации, представляющей персональные данные. d) Обработки информации служебного характера.	ПК-6
	d)	В организационную структуру системы государственного лицензирования в области защиты информации не входят a) ФСБ России; b) ФСТЭК России; ***c) Ростехнадзор;*** ***d) Роскомнадзор;*** e) Лицензионные центры; ***f) Предприятия-заявители.***	ПК-6
	a) c)	Согласно "Положению по аттестации объектов информатизации по требованиям безопасности информации" аттестация объектов информатизации бывает следующих видов **a)** ***Добровольной;*** b) Принудительной; **c)** ***Обязательной;*** d) Заявительной; e) Уведомительной.	ПК-6
	a)	Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров, называется **a)** ***Объектом информатизации;*** b) Объектом автоматизации; c) Криптографической системой;	ПК-6

		d) Информационной системой.	
	a) b) c) d)	В каких случаях аттестация объекта информатизации является обязательной: **a)** ***обработка государственной тайны*;** **b)** ***при защите государственного информационного ресурса*;** **c)** ***при управлении экологически опасными объектами*;** **d)** ***при ведении секретных переговоров*;** e) при обработке коммерческой тайны; при обработке документов ноу-хау.	ПК-6
	a)	На чем основаны специальные методы неформального моделирования комплексной системы защиты информации? **a)** ***На применении неформальной теории систем*;** b) Теории математической связи; c) Теории информации; d) Теории управления.	ПК-6
	a) b) d)	Для чего предназначен стандарт ISO 17799? **a)** ***ISO 17799 может быть использован в качестве критериев для осуществления информационной безопасности организационного уровня, включая административные, процедурные и физические меры защиты*;** **b)** ***Для сертификации организации*;** c) ISO 17799 может быть использован в качестве критериев для осуществления управления информационной безопасностью.	ПК-6
	a)	По документам ГТК самый низкий класс защищенности СВТ от НСД к информации **a)** ***6*;** b) 1; c) 0; d) 9.	ПК-6
	b)	Какие из перечисленных стандартов являются Стандартами управления информационной безопасностью? a) Международные стандарты BS 7799 и ISO/IEC 17799; ***b) Международный стандарт ISO/IEC 27001;*** c) Международный стандарт ISO/IEC 15408.	ПК-6

	b)	Какие из перечисленных стандартов являются Стандартами управления информационной безопасностью? a) Международные стандарты BS 7799 и ISO/IEC 17799; ***b) Международный стандарт ISO/IEC 27001;*** c) Международный стандарт ISO/IEC 15408.	ПК-6
	a)	По документам ГТК самый низкий класс защищенности СВТ от НСД к информации **a) *6*;** b) 1; c) 0; d) 9.	ПК-6
	a)	На чем основаны специальные методы неформального моделирования комплексной системы защиты информации? **a) *На применении неформальной теории систем*;** b) Теории математической связи; c) Теории информации; d) Теории управления.	ПК-6
	a) b)	Для чего предназначен стандарт ISO 17799? **a) *ISO 17799 может быть использован в качестве критериев для осуществления информационной безопасности организационного уровня, включая административные, процедурные и физические меры защиты*;** **b) *Для сертификации организации*;** c) ISO 17799 может быть использован в качестве критериев для осуществления управления информационной безопасностью.	ПК-6
	d)	Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности? a) Список стандартов, процедур и политик для разработки программы безопасности; b) Текущая версия ISO 17799; c) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях; ***d) Открытый стандарт, определяющий цели контроля.***	ПК-6

		К правовым методам, обеспечивающим информационную безопасность, относятся: a) Разработка аппаратных средств обеспечения правовых данных; b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий; c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности.	ПК-6
		Что понимается под понятием «Конфиденциальность персональных данных»? a) Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных; b) Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотренное федеральным законом; c) Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.	ПК-6
		Основными рисками информационной безопасности являются: a) Искажение, уменьшение объема, перекодировка информации; b) Техническое вмешательство, выведение из строя оборудования сети; c) Потеря, искажение, утечка информации.	ПК-6
		Основными субъектами информационной безопасности являются: a) руководители, менеджеры, администраторы компаний; b) органы права, государства, бизнеса; c) сетевые базы данных, фаерволлы.	ПК-6
		Наиболее важным при реализации защитных мер политики безопасности является: a) Аудит, анализ затрат на проведение защитных мер; b) Аудит, анализ безопасности; Аудит, анализ уязвимостей, риск-ситуаций.	ПК-6
		Согласно "Положению по аттестации объектов информатизации по требованиям безопасности информации" аттестация объектов информатизации бывает следующих	ПК-6

		видов a) Добровольной; b) Принудительной; c) Обязательной; d) Заявительной; e) Уведомительной.	
		Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров, называется a) Объектом информатизации; b) Объектом автоматизации; c) Криптографической системой; d) Информационной системой.	ПК-6
		В каких случаях аттестация объекта информатизации является обязательной: a) обработка государственной тайны; b) при защите государственного информационного ресурса; c) при управлении экологически опасными объектами; d) при ведении секретных переговоров; e) при обработке коммерческой тайны; f) при обработке документов ноу-хау.	ПК-6
		На чем основаны специальные методы неформального моделирования комплексной системы защиты информации? a) На применении неформальной теории систем; b) Теории математической связи; c) Теории информации; d) Теории управления.	ПК-6
		Для чего предназначен стандарт ISO 17799? a) ISO 17799 может быть использован в качестве критериев для осуществления информационной безопасности организационного уровня, включая административные, процедурные и физические меры защиты;	ПК-6

		b) Для сертификации организации; c) ISO 17799 может быть использован в качестве критериев для осуществления управления информационной безопасностью.	
		Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности? a) Список стандартов, процедур и политик для разработки программы безопасности; b) Текущая версия ISO 17799; c) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях; d) Открытый стандарт, определяющий цели контроля.	ПК-6
		По документам ГТК самый низкий класс защищенности СВТ от НСД к информации a) 6; b) 1; c) 0; d) 9.	ПК-6
		Какие из перечисленных стандартов являются Стандартами управления информационной безопасностью? a) Международные стандарты BS 7799 и ISO/IEC 17799; b) Международный стандарт ISO/IEC 27001; c) Международный стандарт ISO/IEC 15408.	ПК-6
	d)	Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности? a) Список стандартов, процедур и политик для разработки программы безопасности; b) Текущая версия ISO 17799; c) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях; ***d) Открытый стандарт, определяющий цели контроля.***	ПК-6
		Цели и задачи дисциплины «Аттестация объектов информационной безопасности».	ПК-6

		Дайте определение информации в соответствии с Федеральным законом Российской Федерации "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ.	ПК-6
		Дайте определение общедоступной информации. Виды общедоступной информации и их характеристика.	ПК-6
		Дайте определение информации ограниченного использования. Виды информации ограниченного использования и их характеристика.	ПК-6
		Дайте определение государственной тайны. Особенности защиты информации, относящейся к государственной тайне и информации ограниченного использования.	ПК-6
		Дайте определение объекта информатизации.	ПК-6
		Дайте определение объекта информатизации, аттестуемого по требованиям безопасности информации.	ПК-6
		Система аттестации объектов информатизации по требованиям безопасности информации России.	ПК-6
		Охарактеризуйте органы исполнительной власти, уполномоченные в области безопасности информации.	ПК-6
		Перечислите основные нормативно-методические документы, регламентирующие порядок проведения аттестации объектов информатизации и содержащие требования к объектам информатизации в России.	ПК-6
		Дайте характеристику государственной системы защиты информации (определение, структура, функциональные подсистемы).	ПК-6
		Охарактеризуйте подсистему сертификации средств защиты информации по требованиям безопасности информации.	ПК-6
		Дайте понятие сертификат соответствия, его назначение и порядок использования.	ПК-6
		Охарактеризуйте подсистему лицензирования в области защиты информации.	ПК-6
		Дайте понятие лицензии, ее назначение и порядок использования.	ПК-6
		Охарактеризуйте процесс аттестации объектов информатизации по требованиям безопасности информации.	ПК-6
		Дайте понятие аттестата соответствия, его назначение и порядок использования.	ПК-6
		Охарактеризуйте организационные и технические мероприятия по защите информации, проводимые в рамках выполнения работ по аттестации объектов информатизации.	ПК-6
		Что включает в себя государственный контроль и надзор за соблюдением порядка аттестации объектов информатизации?	ПК-6
		В каких случаях и кем в ходе проверки принимается решение об аннулировании	ПК-6

		«Аттестата соответствия объекта информатизации по требованиям безопасности информации»?	
		Дайте характеристику государственной системы защиты информации (определение, структура, функциональные подсистемы).	ПК-6
		Охарактеризуйте основные виды аттестации объектов информатизации по требованиям безопасности информации.	ПК-6
		Опишите перечень работ при аттестации, проводимый органом по аттестации.	ПК-6
		Опишите функции органа по аттестации и ФСТЭК в процессе аттестации объектов информатизации по требованиям безопасности информации.	ПК-6
		Опишите функции испытательных лабораторий и заказчиков в процессе аттестации объектов информатизации по требованиям безопасности информации.	ПК-6
		Приведите перечень документов и данных, предоставляемых органу по аттестации заявителем для проведения испытаний.	ПК-6
		Приведите общий объем исходных данных и документации, определяемые заявителем для аттестуемого объекта информатизации.	ПК-6
		Охарактеризуйте основные этапы проведения аттестации объектов информатизации по требованиям безопасности информации.	ПК-6
		Охарактеризуйте перечень данных, содержащихся в аттестате соответствия.	ПК-6
		Охарактеризуйте основные разделы приказа руководителя организации о назначении должностного лица или структурного подразделения, ответственного за обеспечение безопасности информации в организации.	ПК-6
		Приведите перечень подготовительных мероприятий, реализуемых заявителем до начала проведения работ по аттестации объектов информатизации по требованиям безопасности.	ПК-6
		Порядок и содержание перечня сведений конфиденциального характера организации, составляемого заявителем.	ПК-6
		Порядок определения условий расположения автоматизированной системы и (или) защищаемого помещения относительно границ контролируемой зоны и основное содержание приказа «Об определении границ контролируемой зоны».	ПК-6
		Обобщенная схема проведения аттестации объекта информатизации по требованиям безопасности информации.	ПК-6
		Перечислите документы, на основании которых органом по аттестации проводятся аттестационные испытания.	ПК-6
		Способы предварительного ознакомления с аттестуемым объектом органом по аттестации.	ПК-6
		Перечень работ, проводимых органом по аттестации в рамках предварительного	ПК-6

		ознакомления с объектом информатизации, подлежащим аттестации.	

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***