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 объектов критической информационной инфраструктуры
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 «Защита объектов критической информационной инфраструктуры» 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) «Защита объектов критической информационной инфраструктуры» 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) Жук А.П., профессор кафедры

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены комиссии: Рачков В.Е., доцент кафедры
Минкина Т.В., доцент кафедры

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

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 объектов критической информационной инфраструктуры».

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,e	Объекты и субъекты КИИ. Права и обязанности субъектов КИИ. a) Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели b) Российские юридические лица и/или индивидуальные предприниматели, которые обеспечивают взаимодействие систем и/или сетей, принадлежащих субъектам КИИ c) Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств d) Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники e) Автоматизированная система управления. Один из видов автоматизированных систем f) Нет верного ответа	ПК-6
2.	A, B	Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. a) Утечка конфиденциальной информации b) Несанкционированный обмен информацией c) Санкционированное использование информационных ресурсов	ПК-6
3.	A,B	Какие есть методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей.? a) Анализ возможных уязвимостей программных, программно-аппаратных средств информационной системы b) Оценка потенциала опасности нарушителей на основе метода главных компонентов c) Цвет одежды нарушителя	ПК-6

		d) Физическая форма внутреннего нарушителя	
4.	D	Напишите перечень показателей критериев значимости объектов КИИ Российской Федерации и их значения. a) Количество населения, обслуживаемого объектом КИИ. b) Территория, на которой функционирует объект КИИ. c) Значимость объекта КИИ для обеспечения функционирования объектов критической информационной инфраструктуры других субъектов КИИ. d) Все варианты верны e) Все варианты неверны	ПК-6
5.	e	Что входит в Реестр значимых объектов КИИ? a) информационные системы b) телекоммуникационные сети c) банковская сфера d) топливно-энергетический комплекс e) все варианты верны	ПК-6
6.	A,B,C	Напишите требования к созданию систем безопасности значимых объектов КИИ? a) Определение целей и задач обеспечения безопасности значимых объектов КИИ b) Разработка модели угроз и категорий нарушителей безопасности информации c) Создание и функционирование системы безопасности d) Подбор правильного персонала e) Обеспечение анонимности	ПК-6
7.	E	Напиши перечень необходимых документов в рамках создания систем безопасности значимых объектов КИИ a) Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации b) Порядок утверждения Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации c) Порядок утверждения правил категорирования объектов критической информационной инфраструктуры Российской Федерации и их значений d) Требования к созданию систем безопасности значимых объектов	ПК-6

		критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования e) Все варианты верны f) Все варианты неверны	
8.	B	Какое будет наказание за нарушение законодательства о безопасности КИИ Российской Федерации? a) Уголовная ответственность b) Административная ответственность c) Ни один из вариантов	ПК-6
9.	A,B,C,D	Какие компьютерные инциденты могут возникнуть в значимых объектах КИИ? a) Взрывы или потеря данных. b) Проблемы с доступом к информации. c) Атаки на критическую информацию. d) Проблемы с отслеживаемостью и мониторингом. e) Ни один из вариантов	ПК-6
10.	A,B,C	Какие программные средства защиты информации существуют? a) Встроенные средства защиты. b) Программы-антивирусы. c) Средства контроля доступа. d) Специалист по защите информации.	ПК-3
11.	A, B, C, D	Требования к обеспечению безопасности включаются в техническое задание на создание значимого объекта и (или) техническое задание на создание подсистемы безопасности значимого объекта, которые должны содержать: a) Цель и задачи обеспечения безопасности значимого объекта или подсистемы безопасности значимого объекта; b) Категорию значимости значимого объекта; c) Перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект; d) Перечень типов объектов защиты значимого объекта; e) Сведения о технических характеристиках оборудования, используемого для обеспечения безопасности значимого объекта или подсистемы безопасности значимого объекта.	ПК-3

		f) Все вышеперечисленное	
12.	D	Основанием для осуществления внеплановой проверки в области обеспечения безопасности значимых объектов критической информационной инфраструктуры является: a) Истечение срока выполнения субъектом критической информационной инфраструктуры выданного ФСТЭК России предписания об устранении выявленного нарушения требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры; b) Возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте критической информационной инфраструктуры; c) Приказ (распоряжение) руководителя ФСТЭК России, изданный в соответствии с поручением Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям; d) Все перечисленные выше основания.	ПК-3
13.	C	Категорирование объекта критической инфраструктуры осуществляется исходя из: a) социальной значимости; политической значимости; финансово-экономической значимости; политической значимости; экологической значимости; значимости объекта для обороны страны; b) социальной значимости; политической значимости; экономической значимости; политической значимости; экологической значимости; значимости объекта для обороны страны; c) социально-политической значимости; информационной значимости; финансово-экономической значимости; политической значимости; экологической значимости; значимости объекта для обеспечения обороны страны, безопасности государства и правопорядка.	ПК-3
14.		Какие организационные меры используются при управлении ИБ? a) Координация действий по защите информации	ПК-3

		b) Независимый анализ информационной безопасности	
15.		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 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	ПК-3
16.		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
17.		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***