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

Методы и средства защиты информации в банковских системах
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. Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Методы и средства защиты информации в банковских системах» 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) «Методы и средства защиты информации в банковских системах» 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) Минкина Т.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 «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 «Методы и средства защиты информации в банковских системах».

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-1. Способен обеспечивать защиту от НСД сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации				
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-1 ПК-1 Способен проводить мониторинг функционирования СССЭ, защищённости от НСД сооружений и СССЭ*	Не может применять методы контроля функционирования СССЭ, их защищенности от НСД Не может проводить анализ средств мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты СССЭ от НСД	Затрудняется применять методы контроля функционирования СССЭ, их защищенности от НСД Анализирует не все средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты СССЭ от НСД	В целом умеет применять в основном все методы контроля функционирования СССЭ, их защищенности от НСД Анализирует в основном все средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты СССЭ от НСД	Грамотно применяет методы контроля функционирования СССЭ, их защищенности от НСД Анализирует средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты СССЭ от НСД

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
1.	a	Потенциальные угрозы, против которых направлены технические меры защиты информации a) 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 и оснащение помещений замками. d) Потери информации из-за не достаточной установки сигнализации в помещении. e) Процессы преобразования, при котором информация удаляется	ПК -1
2.	abc	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; e) аудит на соответствие стандартам менеджмента и качества.	ПК -1
3.	d	Государственную тайну составляют, сведения в области внешней политики и экономики: a) сведения о банках, в которых содержатся счета организации; b) о сотрудничестве с иностранными организациями; c) обобщенные показатели по внешней задолженности; d) о финансовой политике в отношении иностранных государств.	ПК -1
4.	a	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	ПК -1

		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.	
5.	abcdefg	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 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; методика оценки угроз.	ПК -1
6.	a	Оценка рисков позволяет ответить на следующие вопросы: a) чем рискует организация, используя информационную систему?	ПК -1

		b) чем рискуют пользователи информационной системы? c) чем рискуют системные администраторы?	
7.	a	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
8.	abc	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; e) аудит на соответствие стандартам менеджмента и качества.	ПК -1
9.	a	Разработка и внедрение новых информационно-вычислительных систем, в рамках которых решается весь комплекс проблем защиты информации это a) креативный подход; b) аддитивный подход; интеграционный подход.	ПК -1
10.	c	Наиболее важным при реализации защитных мер политики безопасности является: a) Аудит, анализ затрат на проведение защитных мер b) Аудит, анализ безопасности c) Аудит, анализ уязвимостей, риск-ситуаций	ПК -1
11.		Для чего проводят технико-экономическое обоснование средств защиты? Для … (в родительном падеже)	ПК -1

		(Ответ: для анализа и оценки целесообразности реализации применяемых средств).	
12.	a	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; контроль и проверка процессов систем пожарной сигнализации.	
13.	a	Виды информационной безопасности: a) персональная, корпоративная, государственная; b) клиентская, серверная, сетевая; c) локальная, глобальная, смешанная	ПК -1
14.	abfg	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
15.	b	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

16.	abc	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
17.	bc	Какие свойства информации выполняет резервное копирование? a) конфиденциальность; b) целостность; c) доступность.	ПК -1
18.		Основы кредитно-банковской системы России	ПК -1
19.		Платежная система и межбанковские расчеты	ПК -1
20.		Традиционная и электронная коммерции. Виды электронной коммерции.	ПК -1
21.		Типы дематериализованных денег. Электронные кошельки	ПК -1
22.		Факторы, влияющие на безопасность в банковской сфере.	ПК -1
23.		Классификация угроз.	ПК -1
24.		Состав и структура системы безопасности банка.	ПК -1
25.		Понятие и модели политики безопасности.	ПК -1
26.		Механизмы защиты.	ПК -1
27.		Принципы организации и контроля функционирования автоматизированных сетей.	ПК -1
28.		Опасные события и их предупреждение.	ПК -1
29.		Устранение нарушений. Дополнительные меры контроля.	ПК -1
30.		Обмен электронными данными. Торговые расчеты. Межбанковские расчеты. Основные способы межбанковских платежей.	ПК -1
31.		Общие проблемы безопасности электронного обмена данных.	ПК -1
32.		Классификация типов мошенничества в электронной коммерции.2.Протокол SSL.	ПК -1
33.		Система сообщества всемирных межбанковских финансовых телекоммуникаций	ПК -1
34.		(SWIFT).	ПК -1

35.		Клиринговая система CHAPS.	ПК -1
36.		Концепция безопасности банка.	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».

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если в совершенстве формулирует понятия информации, информационной безопасности, Способен проводить мониторинг функционирования СССЭ, защищённости от НСД сооружений и СССЭ

Оценка «хорошо» выставляется студенту, если формулирует понятия информации, информационной безопасности, способен проводить мониторинг функционирования СССЭ, защищённости от НСД сооружений и СССЭ

Оценка «удовлетворительно» выставляется студенту, если слабо формулирует понятия информации, информационной безопасности, Способен проводить мониторинг функционирования СССЭ, защищённости от НСД сооружений и СССЭ

Оценка «неудовлетворительно» выставляется студенту, если не формулирует понятия информации, способен проводить мониторинг функционирования СССЭ, защищённости от НСД сооружений и СССЭ

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**