МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. директора института
перспективной инженерии,
канд. техн. наук, доцент
А.А. Порохня

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ»

Направление подготовки	11.03.02 Инфокоммуникационные технологии и системы связи
Направленность (профиль)	Интеллектуальная обработка данных в инфокоммуникационных системах и сетях
Год начала обучения	2026
Форма обучения	очно-заочная
Реализуется в семестре	6

Введение

1. Назначение

Фонд оценочных средств по дисциплине «Основы информационной безопасности информационно-коммуникационных систем» предназначен для объективной оценки уровня сформированности компетенций.

2. ФОС является приложением к программе дисциплины «Основы информационной безопасности информационно-коммуникационных систем».

3. Разработчик О.Х. Шаяхметов, доцент департамента цифровых, робототехнических систем и электроники института перспективной инженерии.

4. Проведена экспертиза ФОС.

Члены экспертной группы:
Председатель: В.П. Мочалов, профессор департамента цифровых, робототехнических систем и электроники института перспективной инженерии.
Члены комиссии:
С.В. Яковлев, доцент департамента цифровых, робототехнических систем и электроники института перспективной инженерии.
С.В. Мельников, старший научный сотрудник междисциплинарного учебно-исследовательского центра агротехнологий, доцент департамента цифровых, робототехнических систем и электроники института перспективной инженерии.

Представитель организации работодателя:
Миронов В.А., генеральный директор ООО «Оринтекс».

Экспертное заключение: ФОС по дисциплине позволяет оценить уровень сформированности компетенций. Приступить к апробации.

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 компетенци(ий),			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ПК-7. Способен к администрированию средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)				
ИД-1$_{ПК-7}$ понимает и использует основные принципы, протоколы и программные криптографические средства обеспечения информационной безопасности сетевых устройств.	Не может выполнить задачи, относящиеся к данному индикатору достижения компетенции	Выполняет на репродуктивном уровне задачи, относящиеся к данному индикатору достижения компетенции	Выполняет в стандартных ситуациях задачи, относящиеся к данному индикатору достижения компетенции, допуская незначительные ошибки	Выполняет в полном объеме задачи, относящиеся к данному индикатору достижения компетенции, в том числе в нестандартных ситуациях
ИД-2$_{ПК-7}$ понимает общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем.	Не может выполнить задачи, относящиеся к данному индикатору достижения компетенции	Выполняет на репродуктивном уровне задачи, относящиеся к данному индикатору достижения компетенции	Выполняет в стандартных ситуациях задачи, относящиеся к данному индикатору достижения компетенции, допуская незначительные ошибки	Выполняет в полном объеме задачи, относящиеся к данному индикатору достижения компетенции, в том числе в нестандартных ситуациях
ИД-3$_{ПК-7}$ применяет программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа;	Не может выполнить задачи, относящиеся к данному индикатору достижения компетенции	Выполняет на репродуктивном уровне задачи, относящиеся к данному индикатору достижения компетенции	Выполняет в стандартных ситуациях задачи, относящиеся к данному индикатору достижения компе-	Выполняет в полном объеме задачи, относящиеся к данному индикатору достижения

настраивает параметры современных программно-аппаратных межсетевых экранов.			тенции, допуская незначительные ошибки	компетенции, в том числе в нестандартных ситуациях
ИД-4$_{ПК-7}$ подключает и настраивает современные средства обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов); работает с контрольно-измерительными аппаратными и программными средствами.	Не может выполнить задачи, относящиеся к данному индикатору достижения компетенции	Выполняет на репродуктивном уровне задачи, относящиеся к данному индикатору достижения компетенции	Выполняет в стандартных ситуациях задачи, относящиеся к данному индикатору достижения компетенции, допуская незначительные ошибки	Выполняет в полном объеме задачи, относящиеся к данному индикатору достижения компетенции, в том числе в нестандартных ситуациях
ИД-5$_{ПК-7}$ выполняет установку дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация.	Не может выполнить задачи, относящиеся к данному индикатору достижения компетенции	Выполняет на репродуктивном уровне задачи, относящиеся к данному индикатору достижения компетенции	Выполняет в стандартных ситуациях задачи, относящиеся к данному индикатору достижения компетенции, допуская незначительные ошибки	Выполняет в полном объеме задачи, относящиеся к данному индикатору достижения компетенции, в том числе в нестандартных ситуациях

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
Форма обучения очная Семестр 6			
1.	в	Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена; б) Высшее руководство; в) Владелец; г) Пользователь	ПК -7
2.	а	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? а) Сотрудники; б) Хакеры; в) Атакующие; г) Контрагенты (лица, работающие по договору)	ПК -7
3.	в	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования; б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации; в) Улучшить контроль за безопасностью этой информации; г) Снизить уровень классификации этой информации	ПК -7
4.	б	Что самое главное должно продумать руководство при классификации данных? а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным; б) Необходимый уровень доступности, целостности и конфиденциальности; в) Оценить уровень риска и отменить контрмеры; г) Управление доступом, которое должно защищать данные	ПК -7
5.	г	Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? а) Владельцы данных; б) Пользователи; в) Администраторы; г) Руководство	ПК -7
6.	в	К правовым методам, обеспечивающим информационную безопасность, относятся: а) Разработка аппаратных средств обеспечения правовых данных; б) Разработка и	ПК -7

		установка во всех компьютерных правовых сетях журналов учета действий; в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности	
7.	б	Основными источниками угроз информационной безопасности являются все указанное в списке: а) Хищение жестких дисков, подключение к сети, инсайдерство; б) Перехват данных, хищение данных, изменение архитектуры системы; в) Хищение данных, подкуп системных администраторов, нарушение регламента работы	ПК -7
8.	а	Цели информационной безопасности – своевременное обнаружение, предупреждение: а) несанкционированного доступа, воздействия в сети; б) инсайдерства в организации; в) чрезвычайных ситуаций	ПК -7
9.	а	Основные объекты информационной безопасности: а) Компьютерные сети, базы данных; б) Информационные системы, психологическое состояние пользователей; в) Бизнес-ориентированные, коммерческие системы	ПК -7
10.	в	Основными рисками информационной безопасности являются: а) Искажение, уменьшение объема, перекодировка информации; б) Техническое вмешательство, выведение из строя оборудования сети; в) Потеря, искажение, утечка информации	ПК -7
11.	а	К основным принципам обеспечения информационной безопасности относится: а) Экономической эффективности системы безопасности; б)- Многоплатформенной реализации системы; в) Усиления защищенности всех звеньев системы	ПК -7
12.	б	Основными субъектами информационной безопасности являются: а) руководители, менеджеры, администраторы компаний; б) органы права, государства, бизнеса; в) сетевые базы данных, фаерволлы	ПК -7
13.	а	К основным функциям системы безопасности можно отнести все перечисленное: а) Установление регламента, аудит системы, выявление рисков; б) Установка новых офисных приложений, смена хостинг-компании; в) Внедрение аутентификации, проверки контактных данных пользователей	ПК -7
14.	а	Принципом информационной безопасности является принцип недопущения: а) Неоправданных ограничений при работе в сети (системе); б) Рисков безопасности сети, системы; в) Презумпции секретности	ПК -7
15.	б)	Принципом политики информационной безопасности является принцип:	ПК -7

		а) Невозможности миновать защитные средства сети (системы); б) Усиления основного звена сети, системы; в) Полного блокирования доступа при риск-ситуациях	
16.		Понятие информационной безопасности. Основные составляющие информационной безопасности.	ПК -7
17.		Основные понятия об угрозах.	ПК -7
18.		Законодательный уровень информационной безопасности.	ПК -7
19.		Стандарты и спецификации в области информационной безопасности.	ПК -7
20.		Административный уровень информационной безопасности.	ПК -7
21.		Процедурный уровень информационной безопасности.	ПК -7
22.		Основные понятия программно-технического уровня информационной безопасности.	ПК -7
23.		Архитектура системы безопасности.	ПК -7
24.		Основные принципы криптографической зашиты информации.	ПК -7
25.		Асимметричные криптосистемы.	ПК -7
26.		Симметричные криптосистемы.	ПК -7
27.		Основные понятия и классификация вредоносных программ. Основы борьбы с вредоносными программами.	ПК -7
28.		Типовые удаленные атаки в глобальных компьютерных сетях.	ПК -7
29.		Что включают в себя инженерно-технические средства защиты информации?	ПК -7
30.		Обеспечение безопасности систем входящих в состав глобальных компьютерных сетей.	ПК -7

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 он выполняет в полном объеме и безошибочно задания оценочных средств по дисциплине, относящиеся к данной компетенции (индикаторам достижения компетенции), при этом демонстрирует на высоком уровне способность решать стандартные и нестандартные прикладные практические задачи в области информационной безопасности в инфокоммуникационных системах.

Оценка «хорошо» выставляется студенту, если он выполняет, допуская незначительные ошибки, задания оценочных средств по дисциплине, относящиеся к данной компетенции (индикаторам достижения компетенции), при этом демонстрирует на среднем уровне способность решать только стандартные прикладные практические задачи в области информационной безопасности в инфокоммуникационных системах.

Оценка «удовлетворительно» выставляется студенту, если он выполняет, допуская ошибки, исправление которых осуществляет с помощью наводящих вопросов преподавателя, задания оценочных средств по дисциплине, относящиеся к данной компетенции (индикаторам достижения компетенции), при этом демонстрирует на минимальном уровне способность решать стандартные прикладные практические в области информационной безопасности в инфокоммуникационных системах.

Оценка «неудовлетворительно» выставляется студенту, если он, выполняя задания оценочных средств по дисциплине, не достигает минимального уровня сформированности компетенции (индикаторам достижения компетенции), при этом не демонстрирует способность решать стандартные прикладные практические задачи в области информационной безопасности в инфокоммуникационных системах, допускает грубые ошибки, которые не может исправить даже с помощью наводящих вопросов преподавателя.