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
Порохня А.А.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Основы информационной безопасности и защиты информации

Направление подготовки	11.03.04 Электроника и наноэлектроника
Направленность (профиль)	Интеллектуальные программируемые системы и устройства
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	4

Введение

1. Назначение

Фонд оценочных средств по дисциплине «Основы информационной безопасности и защиты информации» предназначен для формирования у студентов направления подготовки 11.03.04 Электроника и наноэлектроника общепрофессиональных компетенций.

Фонд оценочных средств текущей и промежуточной аттестации разработан на основе рабочей программы «Основы информационной безопасности информационно-коммуникационных систем» и в соответствии с образовательной программой по направлению подготовки 11.03.04 Электроника и наноэлектроника.

ФОС является приложением к программе дисциплины (модуля) по направлению подготовки 11.03.04 Электроника и наноэлектроника.

2. Разработчик (и) Шаяхметов О.Х., доцент департамента ЦРСиЭ

3. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель Г.И. Линец, профессор департамента ЦРСиЭ.
(*Ф.И.О., должность*)
Члены комиссии: В.И. Никулин, доцент департамента ЦРСиЭ;
(*Ф.И.О., должность*)
С.В. Яковлев, доцент департамента ЦРСиЭ.
(*Ф.И.О., должность*)

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

Экспертное заключение фонд оценочных средств соответствует ОП ВО по направлению подготовки 11.03.04 Электроника и наноэлектроника и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Основы информационной безопасности и защиты информации».

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: ОПК-3. Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности				
ИД-4$_{ОПК-3}$ Обеспечивает информационную безопасность при использовании информационных технологий в профессиональное деятельности	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	Понимает и использует основные принципы, протоколы и программные криптографические средства обеспечения информационной безопасности информационно-коммуникационных систем.
Компетенция ОПК-4. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности				
ИД-5$_{ОПК-4}$ Решает конкретные задачи профессиональной деятельности с помощью современных программных средств	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	Применяет программные, аппаратные и программно-аппаратные средства защиты устройств от несанкционированного доступа.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения очная Семестр 3	
1.	в	Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена; б) Высшее руководство; в) Владелец; г) Пользователь	ОПК-3, ОПК-4
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)	ОПК-3, ОПК-4
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	ОПК-3, ОПК-4
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	ОПК-3, ОПК-4
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	ОПК-3, ОПК-4
6.	в	К правовым методам, обеспечивающим информационную безопасность, относятся: а) Разработка аппаратных средств обеспечения правовых данных; б) Разработка и	ОПК-3, ОПК-4

		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	ОПК-3, ОПК-4
8.	а	Цели информационной безопасности – своевременное обнаружение, предупреждение: а) несанкционированного доступа, воздействия в сети; б) инсайдерства в организации; в) чрезвычайных ситуаций	ОПК-3, ОПК-4
9.	а	Основные объекты информационной безопасности: а) Компьютерные сети, базы данных; б) Информационные системы, психологическое состояние пользователей; в) Бизнес-ориентированные, коммерческие системы	ОПК-3, ОПК-4
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	ОПК-3, ОПК-4
11.	а	К основным принципам обеспечения информационной безопасности относится: а) Экономической эффективности системы безопасности; б)-Многоплатформенной реализации системы; в) Усиления защищенности всех звеньев системы	ОПК-3, ОПК-4
12.	б	Основными субъектами информационной безопасности являются: а) руководители, менеджеры, администраторы компаний; б) органы права, государства, бизнеса; в) сетевые базы данных, фаерволлы	ОПК-3, ОПК-4
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	ОПК-3, ОПК-4
14.	а	Принципом информационной безопасности является принцип недопущения: а) Неоправданных ограничений при работе в сети (системе); б) Рисков	ОПК-3, ОПК-4

		безопасности сети, системы; в) Презумпции секретности	
15.		Принципом политики информационной безопасности является принцип: а) Невозможности миновать защитные средства сети (системы); б) Усиления основного звена сети, системы; в) Полного блокирования доступа при риск-ситуациях	ОПК-3, ОПК-4
16.		Понятие информационной безопасности. Основные составляющие информационной безопасности.	ОПК-3, ОПК-4
17.		Основные понятия об угрозах.	ОПК-3, ОПК-4
18.		Законодательный уровень информационной безопасности.	ОПК-3, ОПК-4
19.		Стандарты и спецификации в области информационной безопасности.	ОПК-3, ОПК-4
20.		Административный уровень информационной безопасности.	ОПК-3, ОПК-4
21.		Процедурный уровень информационной безопасности.	ОПК-3, ОПК-4
22.		Основные понятия программно-технического уровня информационной безопасности.	ОПК-3, ОПК-4
23.		Архитектура системы безопасности.	ОПК-3, ОПК-4
24.		Основные принципы криптографической зашиты информации.	ОПК-3, ОПК-4
25.		Асимметричные криптосистемы.	ОПК-3, ОПК-4
26.		Симметричные криптосистемы.	ОПК-3, ОПК-4
27.		Основные понятия и классификация вредоносных программ. Основы борьбы с вредоносными программами.	ОПК-3, ОПК-4
28.		Типовые удаленные атаки в глобальных компьютерных сетях.	ОПК-3, ОПК-4
29.		Что включают в себя инженерно-технические средства защиты информации?	ОПК-3, ОПК-4
30.		Обеспечение безопасности систем входящих в состав глобальных компьютерных сетей.	ОПК-3, ОПК-4

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 инфокоммуникационных технологий и систем связи.

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 инфокоммуникационных технологий и систем связи.

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 инфокоммуникационных технологий и систем связи.

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 инфокоммуникационных технологий и систем связи, допускает грубые ошибки, которые не может исправить даже с помощью наводящих вопросов преподавателя.

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