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
«Обеспечение информационной безопасности в инфокоммуникациях»

Направление подготовки	11.04.02 Инфокоммуникационные технологии и системы связи
Направленность (профиль)	Технологии построения программно-управляемых систем и компьютерных сетей
Год начала обучения	2026 г.
Форма обучения	очная
Реализуется в семестре	3

Введение

1. Назначение

Фонд оценочных средств по дисциплине «Обеспечение информационной безопасности в инфокоммуникациях» предназначен для объективной оценки уровня сформированности компетенций.

2. ФОС является приложением к программе дисциплины «Обеспечение информационной безопасности в инфокоммуникациях».

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, индикаторы	Уровни сформированности компетенции			
	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				
ИД-1$_{ОПК-3.1}$ определяет принципы построения локальных и глобальных компьютерных сетей, основы Интернет-технологий, типовые процедуры применения проблемно-ориентированных прикладных программных средств в дисциплинах профессионального цикла и профессиональной сфере 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	Выполняет в полном объеме задачи, относящиеся к данному индикатору достижения компетенции, в том числе в нестандартных ситуациях
ИД-2$_{ОПК-3.2}$ использует современные информационные и компьютерные технологии, средства коммуникаций, способствующие повышению эффективности научной и образовательной сфер 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	Выполняет в полном объеме задачи, относящиеся к данному индикатору достижения компетенции, в том числе в нестандартных ситуациях
ИД-3$_{ОПК-3.3}$ использует передовой отечественный и зарубежный опыт при проведении исследований, проектировании, организации	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

технологических процессов и эксплуатации инфокоммуникационных систем, сетей и устройств и /или их составляющих				

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
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
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
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
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
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
6.	в	К правовым методам, обеспечивающим информационную безопасность, относятся: а) Разработка аппаратных средств обеспечения правовых данных; б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий; в)	ОПК-3

		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
8.	а	Цели информационной безопасности – своевременное обнаружение, предупреждение: а) несанкционированного доступа, воздействия в сети; б) инсайдерства в организации; в) чрезвычайных ситуаций	ОПК-3
9.	а	Основные объекты информационной безопасности: а) Компьютерные сети, базы данных; б) Информационные системы, психологическое состояние пользователей; в) Бизнес-ориентированные, коммерческие системы	ОПК-3
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
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
12.	б	Основными субъектами информационной безопасности являются: а) руководители, менеджеры, администраторы компаний; б) органы права, государства, бизнеса; в) сетевые базы данных, фаерволлы	ОПК-3
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
14.	а	Принципом информационной безопасности является принцип недопущения: а) Неоправданных ограничений при работе в сети (системе); б) Рисков безопасности сети, системы; в) Презумпции секретности	ОПК-3
15.	б)	Принципом политики информационной безопасности является принцип: а) Невозможности миновать защитные средства сети (системы); б) Усиления	ОПК-3

		основного звена сети, системы; в) Полного блокирования доступа при риск-ситуациях	
16.	в	Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена; б) Высшее руководство; в) Владелец; г) Пользователь	ОПК-3
17.	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
18.	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
19.	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
20.	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
21.	в	К правовым методам, обеспечивающим информационную безопасность, относятся: а) Разработка аппаратных средств обеспечения правовых данных; б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий; в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности	ОПК-3
22.	б	Основными источниками угроз информационной безопасности являются все указанное в списке:	ОПК-3

		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	
23.	а	Цели информационной безопасности – своевременное обнаружение, предупреждение: а) несанкционированного доступа, воздействия в сети; б) инсайдерства в организации; в) чрезвычайных ситуаций	ОПК-3
24.	а	Основные объекты информационной безопасности: а) Компьютерные сети, базы данных; б) Информационные системы, психологическое состояние пользователей; в) Бизнес-ориентированные, коммерческие системы	ОПК-3
25.	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
26.	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
27.	б	Основными субъектами информационной безопасности являются: а) руководители, менеджеры, администраторы компаний; б) органы права, государства, бизнеса; в) сетевые базы данных, фаерволлы	ОПК-3
28.	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
29.	а	Принципом информационной безопасности является принцип недопущения: а) Неоправданных ограничений при работе в сети (системе); б) Рисков безопасности сети, системы; в) Презумпции секретности	ОПК-3
30.	а	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
31.	а	К основным принципам обеспечения информационной безопасности относится:	ОПК-3

		а) Экономической эффективности системы безопасности; б)- Многоплатформенной реализации системы; в) Усиления защищенности всех звеньев системы	
32.	б	Основными субъектами информационной безопасности являются: а) руководители, менеджеры, администраторы компаний; б) органы права, государства, бизнеса; в) сетевые базы данных, фаерволлы	ОПК-3
33.	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
34.	а	Принципом информационной безопасности является принцип недопущения: а) Неоправданных ограничений при работе в сети (системе); б) Рисков безопасности сети, системы; в) Презумпции секретности	ОПК-3
35.	а	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
36.	в	Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена; б) Высшее руководство; в) Владелец; г) Пользователь	ОПК-3
37.	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
38.	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
39.	б	Что самое главное должно продумать руководство при классификации данных? а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к	ОПК-3

		данным; б) Необходимый уровень доступности, целостности и конфиденциальности; в) Оценить уровень риска и отменить контрмеры; г) Управление доступом, которое должно защищать данные	
40.	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
41.	в	К правовым методам, обеспечивающим информационную безопасность, относятся: а) Разработка аппаратных средств обеспечения правовых данных; б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий; в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности	ОПК-3
42.	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
43.	а	Цели информационной безопасности – своевременное обнаружение, предупреждение: а) несанкционированного доступа, воздействия в сети; б) инсайдерства в организации; в) чрезвычайных ситуаций	ОПК-3
44.	а	Основные объекты информационной безопасности: а) Компьютерные сети, базы данных; б) Информационные системы, психологическое состояние пользователей; в) Бизнес-ориентированные, коммерческие системы	ОПК-3
45.	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
46.	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
47.		Понятие информационной безопасности. Основные составляющие информационной безопасности.	ОПК-3

48.		Основные понятия об угрозах.	ОПК-3
49.		Законодательный уровень информационной безопасности.	ОПК-3
50.		Стандарты и спецификации в области информационной безопасности.	ОПК-3
51.		Административный уровень информационной безопасности.	ОПК-3
52.		Процедурный уровень информационной безопасности.	ОПК-3
53.		Основные понятия программно-технического уровня информационной безопасности.	ОПК-3
54.		Архитектура системы безопасности.	ОПК-3
55.		Основные принципы криптографической зашиты информации.	ОПК-3
56.		Асимметричные криптосистемы.	ОПК-3
57.		Симметричные криптосистемы.	ОПК-3
58.		Основные понятия и классификация вредоносных программ. Основы борьбы с вредоносными программами.	ОПК-3
59.		Типовые удаленные атаки в глобальных компьютерных сетях.	ОПК-3
60.		Что включают в себя инженерно-технические средства защиты информации?	ОПК-3
61.		Обеспечение безопасности систем входящих в состав глобальных компьютерных сетей.	ОПК-3

2. Описание шкалы оценивания

Успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

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 управления проектами в профессиональной сфере.

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 управления проектами в профессиональной сфере.

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 задачи управления проектами в профессиональной сфере.

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 управления проектами в профессиональной сфере, допускает грубые ошибки, которые не может исправить даже с помощью наводящих вопросов преподавателя.