

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ефанов Алексей Валерьевич

Должность: Директор Невиномысского технологического института (филиал) СКФУ

Дата подписания: 05.03.2024 14:25:49

Уникальный программный ключ:

49214306dd433e7a1b0f8632f645f9d53c99e3d0

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

**УТВЕРЖДАЮ**

Директор НТИ (филиал) СКФУ

Ефанов А.В

ЭЛЕКТРОННЫЙ ДОКУМЕНТ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ**

«Информационная безопасность и защита данных»

Направление подготовки	15.04.04 Автоматизация технологических процессов и производств
Направленность (профиль)	Информационно-управляющие системы
Год начала обучения	2024
Форма обучения	заочная
Реализуется в семестре	5

## Введение

1. Назначение: оценивание уровня сформированности компетенций обучающихся, определенных программой дисциплины «Информационная безопасность и защита данных».

2. ФОС является приложением к программе дисциплины «Информационная безопасность и защита данных».

3. Разработчик: Евдокимов А.А., доцент кафедры информационных систем, электропривода и автоматики, кандидат технических наук, доцент

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:

Мельникова Е.Н., председатель УМК НТИ (филиал) СКФУ

Члены комиссии:

А.И. Колдаев, и.о. зав. кафедрой информационных систем, электропривода и автоматики

Д.В. Болдырев, доцент кафедры информационных систем, электропривода и автоматики

Представитель организации-работодателя:

Остапенко Н.А., к.т.н., ведущий конструктор КИЭП «Энергомера» филиал АО «Электротехнические заводы «Энергомера»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств и рекомендуется для оценивания уровня сформированности компетенций обучающихся, определенных программой дисциплины «Информационная безопасность и защита данных».

« \_\_\_\_ » \_\_\_\_\_ 2024 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

## 1 Описание показателей и критериев оценивания на различных этапах их формирования, описание шкал оценивания

Уровни сформированности компетенци(ий), индикатора(ов)	Дескрипторы			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
<i>Компетенция:</i> ПК-3. Способен собирать и анализировать исходные данные для проектирования средств и систем автоматизации				
Результаты обучения по дисциплине (модулю): <i>Индикатор:</i> ИД-1 <sub>ПК-3</sub> Собирает и анализирует исходные данные для проектирования средств и систем автоматизации	Не умеет собирать и анализировать исходные данные для проектирования средств и систем автоматизации	Демонстрирует ограниченные навыки сбора и анализа исходных данных для проектирования средств и систем автоматизации	Демонстрирует навыки сбора и анализа исходных данных для проектирования средств и систем автоматизации	Способен собирать и анализировать исходные данные для проектирования средств и систем автоматизации
Результаты обучения по дисциплине (модулю): <i>Индикатор:</i> ИД-2 <sub>ПК-3</sub> Оформляет техническое задание и обосновывает его для заказчика	Не умеет оформлять техническое задание и обосновывает его для заказчика	Демонстрирует ограниченное умение оформлять техническое задание и обосновывает его для заказчика	Демонстрирует умение оформлять техническое задание и обосновывает его для заказчика	Способен оформлять техническое задание и обосновывает его для заказчика
Результаты обучения по дисциплине (модулю): <i>Индикатор:</i> ИД-3 <sub>ПК-3</sub> Использует современные информационные технологии для сбора и анализа исходных данных для проектирования средств и систем автоматизации	Не способен использовать современные информационные технологии для сбора и анализа исходных данных для проектирования средств и систем автоматизации	Имеет ограниченные навыки использования современных информационных технологий для сбора и анализа исходных данных для проектирования средств и систем автоматизации	Имеет навыки использования современных информационных технологий для сбора и анализа исходных данных для проектирования средств и систем автоматизации	Способен использовать современные информационные технологии для сбора и анализа исходных данных для проектирования средств и систем автоматизации

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 очно-заочная, семестр 5			
1.	1	Основная масса угроз информационной безопасности приходится на: 1. Троянские программы 2. Шпионские программы 3. Черви	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
2.	3	Конфиденциальностью называется: 1. защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов 2. описание процедур 3. защита от несанкционированного доступа к информации	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
3.	2	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству: 1. снизить уровень классификации этой информации 2. улучшить контроль за безопасностью этой информации 3. требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
4.	3	Что самое главное должно продумать руководство при классификации данных: 1. управление доступом, которое должно защищать данные 2. оценить уровень риска и отменить контрмеры 3. необходимый уровень доступности, целостности и конфиденциальности	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
5.	2	Что такое политика безопасности: 1. детализированные документы по обработке инцидентов безопасности 2. широкие, высокоуровневые заявления руководства 3. общие руководящие требования по достижению определенного уровня безопасности	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
6.	2	Основными источниками угроз информационной безопасности являются все указанное в списке: 1. Хищение жестких дисков, подключение к сети, инсайдерство 2. Перехват данных, хищение данных,	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3

		изменение архитектуры системы 3. Хищение данных, подкуп системных администраторов, нарушение регламента работы	
7.	1	Виды информационной безопасности: 1. Персональная, корпоративная, государственная 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, смешанная	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
8.	1	Цели информационной безопасности – своевременное обнаружение, предупреждение: 1. несанкционированного доступа, воздействия в сети 2. инсайдерства в организации 3. чрезвычайных ситуаций	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
9.	1	Основные объекты информационной безопасности: 1. Компьютерные сети, базы данных 2. Информационные системы, психологическое состояние пользователей 3. Бизнес-ориентированные, коммерческие системы	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
10.	3	Принципом информационной безопасности является принцип недопущения: 1. Рисков безопасности сети, системы 2. Презумпции секретности 3. Неоправданных ограничений при работе в сети (системе)	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
11.	1	Принципом политики информационной безопасности является принцип: 1. Усиления защищенности самого незащищенного звена сети (системы) 2. Перехода в безопасное состояние работы сети, системы 3. Полного доступа пользователей ко всем ресурсам сети, системы	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
12.	2	ЭЦП – это: 1. Электронно-цифровой преобразователь 2. Электронно-цифровая подпись 3. Электронно-цифровой процессор	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
13.	3	Наиболее распространены угрозы информационной безопасности сети: 1. Распределенный доступ клиент, отказ оборудования 2. Моральный износ сети, инсайдерство 3. Сбой (отказ) оборудования, нелегальное копирование данных	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
14.	1	Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: 1. Целостность	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3

		2. Доступность 3. Актуальность	
15.	1	Защита информации – это... 1. комплекс мероприятий, направленных на обеспечение информационной безопасности. 2. процесс разработки структуры базы данных в соответствии с требованиями пользователей 3. небольшая программа для выполнения определенной задачи	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
16.		Какие виды программного обеспечения могут содержать вирусы?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
17.		Какие риски связаны с использованием открытых сетей передачи данных	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
18.		Что такое ботнет и как она может быть использована для атак на компьютеры?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
19.		Что такое двухфакторная аутентификация и как она работает?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
20.		Какие существуют методы защиты персональных данных?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
21.		Какие меры безопасности следует принимать при работе с облачными сервисами?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
22.		Какие типы устройств хранения данных более надежны?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
23.		Что такое бэкап и зачем его делать?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
24.		Какие виды шифрования существуют?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
25.		Что такое фишинг и как его распознать?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
26.		Что такое шифрование и как оно помогает защитить данные?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
27.		Какие меры безопасности следует принимать при использовании социальных сетей?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
28.		Какие правила использования электронной почты помогают избежать утечки данных?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
29.		Что такое DDoS-атака и как ее предотвратить?	ИД-1ПК-3 ИД-2ПК-3

			ИД-3ПК-3
30.		Что такое криптография и как она связана с информационной безопасностью?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
31.		Какие меры безопасности следует принимать при работе с онлайн-банкингом?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
32.		Что такое мошенничество с использованием банковских карт и как его предотвратить?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
33.		Какие меры безопасности следует принимать при работе с USB-накопителями?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
34.		Что такое доменное имя и как его защитить от злоумышленников?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
35.		Какие меры безопасности следует принимать при использовании облачных хранилищ данных?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
36.		Что такое сетевой фильтр и как он помогает защитить компьютер?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
37.		Какие меры безопасности следует принимать при работе с файлами в Интернете?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
38.		Что такое антивирус и зачем он нужен?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
39.		Какие программы помогают защитить компьютер от вирусов и хакеров?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
40.		Какой пароль считается надежным для защиты данных?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
41.		Какие меры безопасности следует принимать при использовании общественных Wi-Fi сетей?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
42.		Что такое взлом и как его предотвратить?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
43.		Какие виды угроз информационной безопасности существуют?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
44.		Что такое информационная безопасность?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-3
45.		Какие меры безопасности следует принимать при использовании мобильных устройств?	ИД-1ПК-3 ИД-2ПК-3 ИД-3ПК-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 положениях, 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 глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

Оценка **«хорошо»** выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

Оценка **«удовлетворительно»** выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.

Оценка **«неудовлетворительно»** выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.