

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Шебзухова Татьяна Александровна

Должность: Директор Пятигорского института (филиал) Северо-Кавказского

федерального университета

Дата подписания: 18.04.2024 15:37:20

Уникальный программный ключ:

d74ce93cd40e39275c3ba2f58486412a1c8ef96f

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ

Зам. директора по учебной работе

Пятигорского института (филиал)

СКФУ

Н.В. Данченко

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Персональная кибербезопасность

Направление подготовки	<u>09.03.02 Информационные системы и технологии</u>	
Направленность (профиль)	<u>Информационные системы и технологии обработки цифрового контента</u>	
Год начала обучения	<u>2024</u>	
Форма обучения	очная	заочная
Реализуется в семестре	<u>1</u>	1

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Персональная кибербезопасность». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информацию о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.
2. ФОС является приложением к программе дисциплины «Персональная кибербезопасность» и в соответствии с образовательной программой высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии.
3. Разработчик: Мишин В.В., доцент кафедры систем управления и информационных технологий, кандидат экономических наук, доцент

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:

Цаплева В.В. – и.о. зав. кафедрой систем управления и информационных технологий

Члены комиссии:

Флоринский О.С. – доцент кафедры систем управления и информационных технологий

Рудакова Т.А. – доцент кафедры систем управления и информационных технологий

Представитель организации-работодателя:

Афанасов Владимир Христофорович - директор ООО «Сателлит»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 09.03.02 Информационные системы и технологии и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Персональная кибербезопасность».

« ____ » _____ 2024 г.

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
<i>Компетенция: ПК-8</i>				
Результаты обучения по дисциплине (модулю): <i>Индикатор:</i> ИД-1.ПК-8 Понимает способы обеспечения требуемого качественного бесперебойного режима работы инфокоммуникационной системы.	Не понимает способы обеспечения требуемого качественного бесперебойного режима работы инфокоммуникационной системы.	Слабо понимает способы обеспечения требуемого качественного бесперебойного режима работы инфокоммуникационной системы.	Хорошо понимает способы обеспечения требуемого качественного бесперебойного режима работы инфокоммуникационной системы.	Отлично понимает способы обеспечения требуемого качественного бесперебойного режима работы инфокоммуникационной системы.
ИД-2.ПК-8 Обеспечивает требуемый качественный бесперебойный режим работы инфокоммуникационной системы.	Не умеет обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы.	Недостаточно хорошо умеет обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы.	Хорошо умеет обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы.	Отлично умеет обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы.

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 <u>ОФО</u> _ Семестр 1, Форма обучения <u>ЗФО</u> _ Семестр 3			
1.	в)	Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство в) Владелец г) Пользователь	ПК-8
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-8
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-8
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-8

5.	г)	<p>Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?</p> <p>а) Владельцы данных б) Пользователи в) Администраторы г) Руководство</p>	ПК-8
6.	б)	<p>Что такое процедура?</p> <p>а) Правила использования программного и аппаратного обеспечения в компании б) Пошаговая инструкция по выполнению задачи в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах г) Обязательные действия</p>	ПК-8
7.	а)	<p>Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?</p> <p>а) Поддержка высшего руководства б) Эффективные защитные меры и методы их внедрения в) Актуальные и адекватные политики и процедуры безопасности г) Проведение тренингов по безопасности для всех сотрудников</p>	ПК-8
8.	г)	<p>Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?</p> <p>а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски б) Когда риски не могут быть приняты во внимание по политическим соображениям в) Когда необходимые защитные меры слишком сложны г) Когда стоимость контрмер превышает ценность актива и потенциальные потери</p>	ПК-8
9.		Несанкционированный доступ и утечка информации.	ПК-8
10.		Виды угроз.	ПК-8
11.		Непреднамеренные угрозы.	ПК-8

12.		Умышленные угрозы.	ПК-8
13.		Косвенные каналы утечки информации.	ПК-8
14.		Непосредственные каналы утечки информации.	ПК-8
15.		Виды организационных мероприятий.	ПК-8
16.		Уровни правового обеспечения информационной безопасности.	ПК-8
17.		Цели инженерно-технической защиты информации.	ПК-8
18.		Основные аппаратные средства защиты информации.	ПК-8
19.		Основные программные средства защиты информации.	ПК-8
20.		Основные требования к комплексной системе защиты информации.	ПК-8
21.		Основные способы несанкционированного доступа к информации в КС.	ПК-8
22.		Уровни возможностей нарушителя.	ПК-8
23.		Параметры политики учетных записей при использовании парольной аутентификации.	ПК-8
24.		Двухфакторная аутентификация с элементами аппаратного обеспечения (диски, карты, маркеры и т.п.).	ПК-8
25.		Процедура парольной инициализации.	ПК-8
26.		Причины, облегчающие нарушителю реализацию угроз безопасности	ПК-8

		информации в распределенных КС.	
27.		Шифрование перестановкой, его достоинства и недостатки.	ПК-8
28.		Шифрование подстановкой (моно- и многоалфавитной), его достоинства и недостатки.	ПК-8
29.		Свойства абсолютно стойкого шифра.	ПК-8
30.		Свойства однонаправленной функции.	ПК-8
31.		Схема использования симметричной КС для создания защищенного канала связи.	ПК-8
32.		Три группы способов аутентификации.	ПК-8

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

Студенту выставляется «зачтено» выставляется студенту, если студент показал прочное и аргументированное знание программного учебного материала дисциплины, при этом поставленные вопросы раскрывает последовательно, четко и логически стройно, в полном исчерпывающем объеме; умеет правильно формулировать, и владеет основными категориями, понятиями и терминами по материалам дисциплины, не допускает при ответе ошибок. Если он осуществляет самостоятельные практические действия по дисциплине; владеет инновационными приемами работы.

Студенту выставляется «не зачтено» выставляется, если студент допускает грубые ошибки при ответе на вопросы по дисциплине, знает на недостаточно высоком уровне материал дисциплины и не в полной мере готов выполнять практические действия по материалам дисциплины.