

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ефанов Алексей Валерьевич

Должность: Директор Невинномысского технологического института (филиал) СКФУ

Дата подписания: 16.06.2023 14:48:22

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.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Персональная кибербезопасность

Направление подготовки/специальность	09.03.02 Информационные системы и технологии
Направленность (профиль)/специализация	Информационные системы и технологии в бизнесе
Год начала обучения	2023
Форма обучения	очная заочная очно-заочная
Реализуется в семестре	1 1

Введение

1. Назначение: для проведения текущего контроля и промежуточной аттестации по дисциплине «Персональная кибербезопасность» Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информации 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 Кочеров Ю.Н. доцент базовой кафедры регионального индустриального парка

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 автоматике

Э.Е. Тихонов, доцент базовой кафедры территории опережающего социально-экономического развития

Представитель организации-работодателя:

Горшков М. Г., директор ООО «Арнест-информационные технологии»

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 «Проектирование и программирование мобильных приложений и систем».

«01» марта 2023 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 (Неудовлетворител ьно) 2 балла	Минимальный уровень (удовлетворител ьно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
ПК-4 Способен разработать архитектуру ИС				
Результаты обучения по дисциплине (модулю): <i>Индикатор:</i> ИД-1 ПК-4 осуществляет разработку стратегии развития информацион ных технологий инфраструкту ры предприятия и управления ее реализацией ИД-2 ПК-4 осуществляет разработку архитектуры ИТ и ИС инфраструкту ры предприятия	На неудовлетворитель ном уровне понимает основные понятия и определения информационной безопасности; На неудовлетворитель ном уровне осуществляет методы защиты информации с применением симметричных алгоритмов шифрования; На неудовлетворитель ном уровне применяет методы защиты информации с применением асимметричных алгоритмов шифрования	Слабо понимает основные понятия и определения информационно й безопасности; Слабо осуществляет методы защиты информации с применением симметричных алгоритмов шифрования; Слабо уровне применяет методы защиты информации с применением асимметричных алгоритмов шифрования	Понимает основные понятия и определения информацион ной безопасности; Осуществляет методы защиты информации с применением симметричны х алгоритмов шифрования; применяет методы защиты информации с применением асимметричн ых алгоритмов шифрования	
Результаты обучения по дисциплине (модулю): <i>Индикатор:</i> ИД-3 ПК-4 осуществляет обоснование архитектуры ИС				Понимает классификаци ю угроз информацион ной безопасности Анализирует методы защиты информации с применением

				методов основанных на разделении данных Применяет математическ ие модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации;
--	--	--	--	---

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
1.	4) О.	Какая из представленных ниже букв по статистике встречается чаще всего в тексте русского языка 1) А; 2) В; 3) G; 4) О.	ПК-2
2.	3) 0,053 - 0,07.	В этом диапазоне лежит взаимный индекс совпадения для символов русского языка 1) 1000-1000000; 2) 1-100; 3) 0,053 - 0,07.	ПК-2
3.	3) XOR.	Используя какую из представленных ниже логических операций, можно зашифровать сообщение 1) OR; 2) AND; 3) XOR.	ПК-2
4.	3) 0 до 186.	Для представленных $p = 11$ и $q = 17$ в каком диапазоне можно зашифровать числа алгоритмом RSA 1) 1 до 1000000; 2) -1000000 до 1000000; 3) 0 до 186.	ПК-2
5.	3) три части.	Для данных, разделенных с помощью схемы Шамира и полинома второго порядка какое минимальное количество частей необходимо для восстановления информации 1) две части; 2) пять частей; 3) три части.	ПК-2
6.	4) персональные данные.	Как называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу?	ПК-2

		1) личные данные; 2) индивидуальные данные; 3) субъективные данные; 4) персональные данные.	
7.	XOR	Используя эту логическую операцию, можно зашифровать сообщение (ответ напишите только используя латинский алфавит в верхнем регистре)	ПК-2
8.	0	Для $a = 1$ и $b = 1$ напишите, чему будет равняться логическое выражение $a \text{ XOR } b$ (ответ может быть только символ)	ПК-2
9.	о	Эта буква по статистике встречается чаще всего в тексте русского языка (ответ только символ в нижнем регистре)	ПК-2
10.	112	Дан ряд простых чисел 2, 3, 5. В ответ впишите результат целочисленного деления числа 7 на указанный ряд. (В ответе числа указать подряд без пробелов и знаков препинания)	ПК-2
11.	10110	Дано сообщение 10001_2 и ключ 00111_2 в двоичной системе счисления. Каков будет результат если применить алгоритм шифрования XOR	ПК-2
12.	XOR	Эта логическая операция является обратимой и ее можно использовать для симметричного шифрования (ответ напишите только используя латинский алфавит в верхнем регистре)	ПК-2
13.	$255 \text{ XOR } 240 = 11111111 \text{ XOR } 11110000 = 15$	Буква «я» в таблице ASCII кодов соответствует числу 255. Рассчитайте какому числу таблицы ASCII будет зашифрованная буква «я» если применить алгоритм XOR и ключ KEY=240	ПК-2
14.	$(p-1)(q-1) = (127-1)(131-1) = 16380$	Даны два простых числа $p = 127$ и $q = 131$ рассчитайте, чему будет равняться функция Эйлера для алгоритма RSA	ПК-2
15.	$7 \bmod 2 = 1$ $7 \bmod 3 = 1$ $7 \bmod 5 = 2$	Дан ряд оснований $p_1 = 2, p_2 = 3, p_3 = 5$. Рассчитайте, чему будут равны остатки от деления целочисленного числа 7 на указанный ряд оснований	ПК-2
16.		Чем шифрование отличается от кодирования?	ПК-2
17.		В чем заключается идея шифра простой замены?	ПК-2
18.		Алфавиты открытого текста и шифротекста совпадают или отличаются?	ПК-2
19.		Как соотносятся частоты появления открытого текста и шифротекста?	ПК-2
20.		Сколько уникальных вариантов ключа можно получить для заданного размера блока	ПК-2
21.		Опишите как получается матрица Виженера.	ПК-2

22.		Опишите методику шифрования текста шифром Виженера.	ПК-2
23.		Опишите методику нахождения длинны ключевого слова.	ПК-2
24.		Опишите методику нахождения ключевого слова если известна его длина.	ПК-2
25.		Опишите методику шифрования с закрытым ключом.	ПК-2
26.		Опишите логическую операцию XOR.	ПК-2
27.		Механизм работы шифрования на основе XOR.	ПК-2
28.		Насколько надежен рассмотренный алгоритм шифрования на основе XOR?	ПК-2
29.		В чем заключается алгоритм RSA?	ПК-2
30.		Для чего и почему используют комбинированные криптоалгоритмы?	ПК-2
31.		В чем заключаются достоинства и недостатки асимметричных алгоритмов?	ПК-2
32.		В чем заключаются достоинства и недостатки симметричных алгоритмов?	ПК-2
33.		Поясните концепцию разбиения данных. Приведите пример.	ПК-2
34.		Поясните концепцию порогового разделения данных. Приведите пример.	ПК-2
35.		Расскажите принцип порогового разделения данных с применением схемы Шамира.	ПК-2
36.		Расскажите принцип порогового разделения данных с применением схемы Блэкли.	ПК-2
37.		Поясните преимущества использование системы остаточных классов для разделения секрета.	ПК-2
38.		Каким образом информация из системы остаточных классов переводится в десятичную систему счисления с применением китайской теоремы об остатках..	ПК-2
39.		Расскажите принцип порогового разделения данных с применением схемы Миньотта.	ПК-2
40.		Расскажите принцип порогового разделения данных с применением схемы Асмута-Блума	ПК-2

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».

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если он понимает классификацию угроз информационной безопасности; анализирует методы защиты информации с применением методов основанных на разделении данных; применяет математические модели схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации;

Оценка «хорошо» выставляется студенту, если понимает основные понятия и определения информационной безопасности; осуществляет методы защиты информации с применением симметричных алгоритмов шифрования; применяет методы защиты информации с применением асимметричных алгоритмов шифрования

Оценка «удовлетворительно» выставляется студенту, если слабо понимает основные понятия и определения информационной безопасности; слабо осуществляет методы защиты информации с применением симметричных алгоритмов шифрования; слабо уровне применяет методы защиты информации с применением асимметричных алгоритмов шифрования

Оценка «неудовлетворительно» выставляется студенту, если он на неудовлетворительном уровне понимает основные понятия и определения информационной безопасности; на неудовлетворительном уровне осуществляет методы защиты информации с применением симметричных алгоритмов шифрования; на неудовлетворительном уровне применяет методы защиты информации с применением асимметричных алгоритмов шифрования