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)

Информационная безопасность

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	6	8	

Введение

1. Назначение: для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине «Информационная безопасность» 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 «Информационная безопасность» 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 автоматики

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 «Информационная безопасность».

«01» марта 2023 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности				
Результаты обучения по дисциплине (модулю): *Индикатор:*	Осознает на недостаточном уровне задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; Решает на недостаточном уровне задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Применяет на недостаточном уровне решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Осознает на минимальном уровне задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; Решает на минимальном уровне задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Применяет на минимальном уровне решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; Решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Понимает средства защиты информации; угрозы безопасности информации в компьютерных системах; Решает основные этапы построения систем безопасности корпоративных систем; Применяет основные этапы создания комплексной системы защиты информации;
Компетенция: ОПК-7 Способен осуществлять выбор платформ и инструментальных				

программно-аппаратных средств для реализации информационных систем				
Результаты обучения по дисциплине (модулю): *Индикатор:*	Понимает на недостаточном уровне предмет и объект защиты информации; краткий обзор современных методов защиты информации; Использует на недостаточном уровне методы функциональной безопасности корпоративных систем; Применяет на недостаточном ровне методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;	Понимает на минимальном уровне предмет и объект защиты информации; краткий обзор современных методов защиты информации; Использует на минимальном уровне методы функциональной безопасности корпоративных систем; Применяет на минимальном ровне методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;	Понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации; Использует методы функциональной безопасности корпоративных систем; применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;	Понимает интегрированную систему информационной безопасности; защита документооборота в вычислительных системах; средства защиты информации; применяет моделирования комплексных систем защиты информации; методы оценки систем защиты информации; применяет навыки создания алгоритмов шифрования с закрытым ключом; криптографические средства защиты;

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 очная Семестр6, Форма обучения заочная семестр 8	
1.	получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа	Какова цель использования генераторов псевдослучайных чисел при поточном шифровании? – формирование открытых ключей – защита информации от всех случайных или преднамеренных изменений – получение «бесконечной» гаммы (ключевой последовательности), располагая относительно малой длиной самого секретного ключа – защита информации от случайных помех при передаче и хранении сжатие информации	ОПК-3 ОПК-7
2.	количеством бит, которое может одновременно храниться в регистре сдвига	Чем определяется разрядность сдвигового регистра с обратной связью? – скоростью работы регистра – температурой окружающей среды – количеством входов в устройстве генерации функции обратной связи количеством бит, которое может одновременно храниться в регистре сдвига	ОПК-3 ОПК-7
3.	односторонней функцией	Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии – функцией Диффи-Хеллмана – односторонней функцией – функцией Эйлера криптографической функцией	ОПК-3 ОПК-7
4.	блочным алгоритмом симметричного шифрования	Алгоритм ГОСТ 28147-89 является – алгоритмом вычисления функции хеширования – блочным алгоритмом асимметричного шифрования – блочным алгоритмом симметричного шифрования алгоритмом формирования электронной цифровой подписи	ОПК-3 ОПК-7

5.	сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока	Что является особенностью использования режима CBC блочного шифра? – одинаковые сообщения при использовании разных векторов инициализации преобразуются в одинаковый шифротекст – сообщение, зашифрованное в данном режиме, можно расшифровать, выбирая блоки шифротекста в произвольном порядке – одинаковые блоки исходного текста преобразуются в одинаковый шифротекст – этот режим работает очень медленно, что практически не позволяет использовать его для обработки больших (> 1 Кбайт) исходных сообщений сообщение, зашифрованное в данном режиме, можно расшифровать только последовательно, начиная с первого блока	ОПК-3 ОПК-7
6.	10000010	Чему равен результат выполнения побитовой операции «сумма по модулю 2» для шестнадцатеричных чисел 0B5 и 37? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид	ОПК-3 ОПК-7
7.	нет	Может ли шифр с конечным ключом быть совершенным? – да, если это алгоритм шифрования с открытым ключом – в зависимости от параметров шифра – нет – да	ОПК-3 ОПК-7
8.	в них для шифрования и расшифрования информации используется один и тот же ключ	Что общего имеют все методы шифрования с закрытым ключом? – в них для шифрования информации используется один ключ, а для расшифрования – другой ключ – в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов – в них для операций шифрования и расшифрования используется два разных ключа – открытый и закрытый в них для шифрования и расшифрования информации используется один и тот же ключ	ОПК-3 ОПК-7

9.	генерации псевдослучайных чисел	Для чего предназначен алгоритм Блюм-Блюма-Шуба (BBS)? – генерации псевдослучайных чисел – для сжатия информации – для формирования открытых ключей для формирования хеш-кода	ОПК-3 ОПК-7
10.	2, 5, 19, 37, 59, 101	Выберите вариант ответа, содержащий только простые числа – 2, 5, 19, 37, 59, 101 – 2, 7, 17, 37, 57, 107 – 2, 5, 19, 37, 59, 133 – 3, 7, 19, 39, 59, 10	ОПК-3 ОПК-7
11.	Разработка и конкретизация правовых нормативных актов обеспечения безопасности	К правовым методам, обеспечивающим информационную безопасность, относятся: – Разработка аппаратных средств обеспечения правовых данных – Разработка и установка во всех компьютерных правовых сетях журналов учета действий Разработка и конкретизация правовых нормативных актов обеспечения безопасности	ОПК-3 ОПК-7
12.	Перехват данных, хищение данных, изменение архитектуры системы	Основными источниками угроз информационной безопасности являются все указанное в списке: – Хищение жестких дисков, подключение к сети, инсайдерство – Перехват данных, хищение данных, изменение архитектуры системы Хищение данных, подкуп системных администраторов, нарушение регламента работы	ОПК-3 ОПК-7
13.	Персональная, корпоративная, государственная	**Виды информационной безопасности:** – Персональная, корпоративная, государственная – Клиентская, серверная, сетевая Локальная, глобальная, смешанная	ОПК-3 ОПК-7
14.		Цели информационной безопасности – своевременное обнаружение, предупреждение: – несанкционированного доступа, воздействия в сети – инсайдерства в организации	ОПК-3 ОПК-7

		чрезвычайных ситуаций	
15.	Компьютерные сети, базы данных	Основные объекты информационной безопасности: – Компьютерные сети, базы данных – Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие системы	ОПК-3 ОПК-7
16.		Что такое LFSR?	ОПК-3 ОПК-7
17.		Как построить псевдослучайный генератор на основе регистра сдвига?	ОПК-3 ОПК-7
18.		На чем базируется стойкость генераторов псевдослучайных чисел, исследованных в лабораторной работе?	ОПК-3 ОПК-7
19.		Как реализовать возведение в степень чисел большой разрядности по большому модулю?	ОПК-3 ОПК-7
20.		Какая информация является конфиденциальной?	ОПК-3 ОПК-7
21.		Что относится к защищаемой информации?	ОПК-3 ОПК-7
22.		Что понимается под политикой безопасности?	ОПК-3 ОПК-7
23.		Что понимается под несанкционированным воздействием на защищаемую информацию?	ОПК-3 ОПК-7
24.		Дайте понятие конфиденциальности, целостности и доступности информации.	ОПК-3 ОПК-7
25.		Что такое симметричное шифрование?	ОПК-3 ОПК-7
26.		В чем особенность блочных шифров?	ОПК-3 ОПК-7
27.		В чем особенность асимметричных систем шифрования?	ОПК-3 ОПК-7
28.		На чем базируется криптостойкость RSA?	ОПК-3 ОПК-7
29.		Как увеличить производительность системы шифрования RSA?	ОПК-3 ОПК-7

30.		Составляющие функциональной безопасности	ОПК-3 ОПК-7
31.		Этапы построения систем безопасности	ОПК-3 ОПК-7
32.		Назначение цифровой подписи.	ОПК-3 ОПК-7
33.		В чем отличие криптосхемы ЭльГамаля от RSA?	ОПК-3 ОПК-7
34.		Почему шифр RSA называется асимметричным?	ОПК-3 ОПК-7
35.		На чем основана стойкость шифра RSA?	ОПК-3 ОПК-7
36.		Что такое цифровой конверт?	ОПК-3 ОПК-7
37.		Опишите общую схему ЭЦП.	ОПК-3 ОПК-7
38.		Каково назначение хеш-функции?	ОПК-3 ОПК-7
39.		Какими свойствами противодействия должна обладать криптографическая хеш-функция?	
40.		Что такое MAC и как он формируется?	
41.		Какие тесты на случайность вам известны?	
42.		Сравните результаты тестов генераторов из первой лабораторной работы с тестами второй работы	
43.		Дайте определение информационной безопасности.	
44.		Какие цели и задачи включает в себя концепция национальной безопасности РФ?	
45.		Перечислите основные виды угроз информационной безопасности РФ.	

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 средства защиты информации; угрозы безопасности информации в компьютерных системах;
решает основные этапы построения систем безопасности корпоративных систем;
применяет основные этапы создания комплексной системы защиты информации;
понимает интегрированную систему информационной безопасности; защита документооборота в вычислительных системах; средства защиты информации;
применяет моделирования комплексных систем защиты информации; методы оценки систем защиты информации;
применяет навыки создания алгоритмов шифрования с закрытым ключом;
криптографические средства защиты;_____
Оценка «хорошо» выставляется студенту, если он
осознает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
решает задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
применяет решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
понимает предмет и объект защиты информации; краткий обзор современных методов защиты информации;
использует методы функциональной безопасности корпоративных систем;
применяет методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;
Оценка «удовлетворительно» выставляется студенту, если он
осознает на минимальном уровне задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
решает на минимальном уровне задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
применяет на минимальном уровне решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

понимает на минимальном уровне предмет и объект защиты информации; краткий обзор современных методов защиты информации;
использует на минимальном уровне методы функциональной безопасности корпоративных систем;
применяет на минимальном ровне методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;
Оценка «неудовлетворительно» выставляется студенту, если он
осознает на недостаточном уровне задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
решает на недостаточном уровне задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
применяет на недостаточном уровне решения задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
понимает на недостаточном уровне предмет и объект защиты информации; краткий обзор современных методов защиты информации;
использует на недостаточном уровне методы функциональной безопасности корпоративных систем;
применяет на недостаточном ровне методы сообщения и шифрования; стеганографии; кодирования; алгоритмы шифрования с открытым ключом;