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 автоматизированных систем

Направление подготовки	15.03.04 Автоматизация технологических процессов и производств		
Направленность (профиль)	Информационно-управляющие системы		
Год начала обучения	2023		
Форма обучения	очная	заочная	очно-заочная
Реализуется в семестре			8

Введение

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

«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: УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач				
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-1 УК-1 Выделяет проблемную ситуацию, осуществляет ее анализ и диагностику на основе системного подхода*	на недостаточном уровне может применять системный подход при анализе проблемной ситуации	на минимальном уровне может применять системный подход при анализе проблемной ситуации	на среднем уровне может применять системный подход при анализе проблемной ситуации	на высоком уровне может применять системный подход при анализе проблемной ситуации
Компетенция: ПК-3. Способен использовать средства и системы автоматизации, контроля, диагностики, испытаний, управления производством, жизненным циклом продукции и ее качеством.				
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-1 ПК-3 Внедряет на производстве современные методы и средства автоматизации в ходе подготовки производства новой продукции, оценивает ее инновационно*	на недостаточном уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации	на минимальном уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные	на среднем уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и	на высоком уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая

го потенциала.		средства защиты информации	прикладное программное обеспечение, а также аппаратные средства защиты информации	системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации

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 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	УК-1 ПК-3
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	УК-1 ПК-3
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	УК-1 ПК-3
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	УК-1 ПК-3

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	УК-1 ПК-3
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	УК-1 ПК-3
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	УК-1 ПК-3
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	УК-1 ПК-3

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	УК-1 ПК-3
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	УК-1 ПК-3
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	УК-1 ПК-3
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	УК-1 ПК-3
13.	Персональная, корпоративная, государственная	Виды информационной безопасности: – Персональная, корпоративная, государственная – Клиентская, серверная, сетевая Локальная, глобальная, смешанная	УК-1 ПК-3
14.		Цели информационной безопасности – своевременное обнаружение, предупреждение: – несанкционированного доступа, воздействия в сети – инсайдерства в организации чрезвычайных ситуаций	УК-1 ПК-3

15.	Компьютерные сети, базы данных	Основные объекты информационной безопасности: – Компьютерные сети, базы данных – Информационные системы, психологическое состояние пользователей Бизнес-ориентированные, коммерческие системы	УК-1 ПК-3
16.		Что такое LFSR?	УК-1 ПК-3
17.		Как построить псевдослучайный генератор на основе регистра сдвига?	УК-1 ПК-3
18.		Какие тесты на случайность вам известны?	УК-1 ПК-3
19.		На чем базируется стойкость генераторов псевдослучайных чисел, исследованных в лабораторной работе?	УК-1 ПК-3
20.		Как реализовать возведение в степень чисел большой разрядности по большому модулю?	УК-1 ПК-3
21.		Сравните результаты тестов генераторов из первой лабораторной работы с тестами второй работы.	УК-1 ПК-3
22.		Что такое прямое криптографическое преобразование?	УК-1 ПК-3
23.		Что такое сеть Фейстеля	УК-1 ПК-3
24.		Какова криптостойкость режима ECB	УК-1 ПК-3
25.		Поясните алгоритм BLOWFISH	УК-1 ПК-3
26.		Что такое симметричное шифрование?	УК-1 ПК-3
27.		В чем особенность блочных шифров?	УК-1 ПК-3
28.		Какова длина ключа блочного шифра?	УК-1 ПК-3
29.		На чем базируется криптостойкость блочного шифра?	УК-1 ПК-3
30.		Какие элементарные операции используются в симметричном шифровании?	УК-1

			ПК-3
31.		В чем особенность асимметричных систем шифрования?	УК-1 ПК-3
32.		На чем базируется криптостойкость RSA?	УК-1 ПК-3
33.		Как увеличить производительность системы шифрования RSA?	УК-1 ПК-3
34.		Какие атаки на систему RSA вам известны?	УК-1 ПК-3
35.		Как противодействовать атакам на систему RSA?	УК-1 ПК-3
36.		Поясните как работает алгоритм ЭльГамаля	УК-1 ПК-3
37.		Поясните как работает алгоритм RSA?	УК-1 ПК-3
38.		Назначение цифровой подписи?	УК-1 ПК-3
39.		В чем отличие криптосхемы ЭльГамаля от RSA?	УК-1 ПК-3
40.		На чем базируется криптостойкость системы ЭльГамаля?	УК-1 ПК-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».

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 на высоком уровне может применять системный подход при анализе проблемной ситуации
на высоком уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации Оценка «хорошо» выставляется студенту, если он на среднем уровне может применять системный подход при анализе проблемной ситуации
на среднем уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации
Оценка «удовлетворительно» выставляется студенту, если он на минимальном уровне может применять системный подход при анализе проблемной ситуации
на минимальном уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации
Оценка «неудовлетворительно» выставляется студенту, если он на недостаточном уровне может применять системный подход при анализе проблемной ситуации
на недостаточном уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации