МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Утверждаю:
Зав. кафедрой компьютерных интеллектуальных технологий проектирования
_____ М.И. Чижов
«21» декабря 2021 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

«Специальные методы информационной безопасности»

Направление подготовки: 09.04.01 Информатика и вычислительная техника

Направленность (профиль): Искусственный интеллект

Квалификация выпускника магистр

Нормативный период обучения 2 года / 2 года и 5 м.

Форма обучения очная / заочная

Год начала подготовки 2022

Разработчик М.В. Паринов

Воронеж – 2021

Процесс изучения дисциплины «Специальные методы информационной безопасности» направлен на формирование следующих компетенций:

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

ПК-2 - Способен участвовать в решении профессиональных проектных задач, выбирать и реализовывать командную роль в работе над проектом в соответствии с приоритетами собственной деятельности

Перечень планируемых результатов обучения и показателей оценивания сформированности компетенций на этапе промежуточной аттестации

№ п/п	Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Тип ОМ**	**Показатели оценивания**
1	УК-1	Знать классификацию причин нарушений безопасности;	Вопросы (тест) к зачету	Полнота знаний
		Уметь сравнительный анализ параметров систем защиты информации	Стандартные задания	Наличие умений
		Владеть навыками выбора корректных средств защиты информации	Прикладные задания	Наличие навыков
2.	ПК-2	Знать современное состояние и тенденции развития методов информационной безопасности; Уметь разрабатывать,		
		выбирать и тестировать программные средства защиты информации Владеть		
		навыками разработки ПО для защиты информации		

ОПИСАНИЕ ПОКАЗАТЕЛЕЙ, КРИТЕРИЕВ И ШКАЛ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА ЭТАПЕ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Показатели оценивания компетенций	**Шкала и критерии оценки уровня сформированности компетенции**			
	Неудовлетворительный	**Минимально допустимый (пороговый)**	**Средний**	**Высокий**
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущены не грубые ошибки.	Уровень знаний в объёме, соответствующем программе подготовки. Допущены некоторые погрешности.	Уровень знаний в объёме, соответствующем программе подготовки
Наличие умений	При выполнении стандартных заданий не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Выполнены типовые задания с не грубыми ошибками. Выполнены все задания, но не в полном объеме (отсутствуют пояснения, неполные выводы)	Продемонстрированы все основные умения. Выполнены все основные задания с некоторыми погрешностями. Выполнены все задания в полном объёме, но некоторые с недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Задания выполнены в полном объеме без недочетов.
Наличие навыков (владение опытом)	При выполнении стандартных заданий не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для выполнения стандартных заданий с некоторыми недочетами.	Продемонстрированы базовые навыки при выполнении стандартных заданий с некоторыми недочетами.	Продемонстрированы все основные умения. Выполнены все основные и дополнительные задания без ошибок и погрешностей. Продемонстрирован творческий подход к решению нестандартных задач.
Характеристика сформированности компетенции	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение.	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству профессиональных задач.	Сформированность компетенций в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных профессиональных задач.	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных профессиональных задач.

ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Вопросы (тестовые задания) для оценки результатов обучения, характеризующих сформированность компетенций

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	
1.	Исторический подход к защите информации в КС.
2.	Информация – предмет защиты.
3.	Информация – объект защиты.
4.	Случайные угрозы информации в КС.
5.	Преднамеренные угрозы информации в КС.
6.	Защита информации в КС от случайных угроз.
7.	Способы повышения надежности и отказоустойчивости КС.
8.	Защита информации в КС от преднамеренных угроз.
ПК-2 - Способен участвовать в решении профессиональных проектных задач, выбирать и реализовывать командную роль в работе над проектом в соответствии с приоритетами собственной деятельности	
1.	Основные способы НСД.
2.	Физическая защита ПЭВМ от НСД.
3.	Как настроить безопасное соединение
4.	Как настроить защиту беспроводной сети
5.	Как настроить защиту SSH
6.	Как настроить парольную защиту
7.	Как настроить VPN
8.	Как настроить HTTPS
9.	Как настроить FTPS
10.	Как настроить коммутатор с защитой информации
11.	Как настроить динамическую маршрутизацию с шифрованием
12.	Как настроить защиту портов устройства
13.	Основные принципы шифрования DES
14.	Основные принципы шифрования AES
15.	Основные принципы шифрования DSA
16.	Основные принципы шифрования на основе шифра Цезаря
17.	Основные принципы шифрования на основе оригинального шифра подстановки
18.	Основные принципы шифрования на основе оригинального шифра перестановки
19.	Отличие обычных и безопасных соединений
20.	Анализ влияния длины ключа на криптостойкость
21.	Анализ современных алгоритмов шифрования

Практические задания для оценки результатов обучения, характеризующих сформированность компетенций

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	
1.	Шифрование-это: ❖ процесс создания алгоритмов шифрования ❖ процесс сжатия информации ❖ **процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется**

2.	В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией? ❖ **при шифровании с помощью ассимметричного алгоритма** ❖ при шифровании с помощью симметричного алгоритма ❖ арбитр необходим всегда
3.	Можно ли отнести слабую аутентификацию к проблемам безопасности? ❖ нет ❖ **да** ❖ в редких случаях
4.	1. Возможно ли расшифровывать информацию без знания ключа? ❖ нет ❖ **да** ❖ в редких случаях
5.	Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый? ❖ **нет** ❖ да ❖ в редких случаях
6.	Характерная черта алгоритма Эль-Гамаля состоит в : ❖ **протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя** ❖ в точной своевременной передаче сообщения ❖ алгоритм не имеет особенностей и идентичен RSA
7.	Аутентификацией называют: ❖ процесс регистрации в системе ❖ способ защиты системы ❖ **процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов**
8.	Аутентификация бывает: ❖статическая ❖устойчивая ❖постоянная ❖**все варианты правильные** ❖правильного варианта нет
9.	Стойкость ключа характеризуется ❖длинной ❖непредсказуемостью ❖ **все варианты правильные** ❖правильного варианта нет
10.	Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе: ❖**на основе произвольно выбранного шифротекста** ❖**на основе произвольно выбранного открытого текста** ❖на основе только шифротекста
ПК-2 - Способен участвовать в решении профессиональных проектных задач, выбирать и реализовывать командную роль в работе над проектом в соответствии с приоритетами собственной деятельности	
1.	Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает: ❖ **со стороны злоумышленника** ❖ со стороны законного отправителя сообщения

	❖ со стороны законного получателя сообщения
2.	Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки? ❖ асимметричный ❖ **Симметричный** ❖ правильного ответа нет
3.	Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется: ❖ шифрование ❖ дешифровка ❖ расшифровка
4.	В каких основных форматах существует симметричный алгоритм? ❖ блока и строки; ❖ **потока и блока;** ❖ потока и данных
5.	Открытым текстом в криптографии называют: ❖ расшифрованный текст ❖ любое послание ❖ **исходное послание**
6.	Какой ключ известен только приемнику? ❖ открытый ❖ **закрытый** ❖ основании какой информации создается сетевой маршрут?
7.	Наука, занимающаяся защитой информации, путем преобразования этой информации это: ❖ криптография ❖ **криптология** ❖ криптоанализ
8.	В каких **шифрах результат шифрования очередного блока зависит только от** него самого и не зависит от других блоков шифруемого массива данных? ❖ в потоковых ❖ **в блочных**
9.	Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это: ❖ шифр функциональных преобразований ❖ шифр замен ❖ **шифр перестановок**
10.	Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется: ❖ **функция шифрования шага преобразования** ❖ **инвариант стандартного шага шифрования**
11.	**Условие,** при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им *массива открытых данных* размера n используется в анализе: ❖**на основе произвольно выбранного шифротекста** ❖**на основе произвольно выбранного открытого текста** ❖правильного ответа нет
12.	Как называется модификация DESa ❖ Triple Des+ ❖ M-506 ❖ Deh
13.	Какие перестановки существуют в стандарте DES ❖ простые+ ❖ расширенные+ ❖ сокращенные+

14.	Сколько существует перестановок в стандарте DES ❖ 3+ ❖ 4 ❖ 2
15.	Зашифрованный файл, хранящийся на логическом диске, который подключается к системе как еще один логический диск – это… ❖ виртуальный контейнер+ ❖ файл ❖ программа
16.	Устройство, дающее статически случайный шум – это… ❖ генератор случайных чисел+ ❖ контроль ввода на компьютер ❖ УКЗД
17.	УКЗД – это… ❖ устройство криптографической защиты данных+ ❖ устройство криптографической заданности данных ❖ нет правильного ответа
18.	Какой ключ используется в шифре ГОСТ ❖ 256-битовый+ ❖ 246-битовый ❖ 356-битовый
19.	Чем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма ❖ отсутствием начальной перестановки и числом циклов шифрования+ ❖ длиной ключа ❖ методом шифрования
20.	Электронной подписью называется… ❖ присоединяемое к тексту его криптографическое преобразование+ ❖ текст ❖ зашифрованный текст