Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю)
«Математические основы защиты информации и информационной безопасности»

Направление подготовки (специальность)
02.04.02 «Фундаментальная информатика и информационные технологии»

Направленность (профиль)
«Интеллектуальные технологии»

Присваиваемая квалификация
Магистр

Форма обучения
Очная

Год набора
2025

Челябинск, 2025 г.

02.04.02 Фундаментальная информатика и информационные технологии, Интеллектуальные технологии, магистр, *Математические основы защиты информации и информационной безопасности*, 2025, очная

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован

Проректор по учебной работе утверждено 24.02.2025 А.А. Саламатов

Ученым советом института информационных технологий

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета института информационных технологий согласовано Ю. В. Петриченко

Заседанием кафедры информационных технологий и экономической информатики

Протокол заседания № 6 от 20.02.2025

И. о. заведующего кафедрой согласовано С.А. Скрипов

Автор (составитель) А.В. Митянина

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1

Содержание

1. Паспорт фонда оценочных средств

Направление подготовки: 02.04.02 Фундаментальная информатика и информационные технологии
Направленность: Интеллектуальные технологии
Дисциплина: Математические основы защиты информации и информационной безопасности
Семестры: 1
Форма промежуточной аттестации: зачёт
Для оценивания результатов обучения используется балльно-рейтинговая система.

2. Перечень формируемых компетенций

Изучение дисциплины «Математические основы защиты информации и информационной безопасности» направлено на формирование компетенций, приведённых в 1.

Таблица 1. Результаты обучения по дисциплине.

Коды компетенции согласно ФГОС (ОПОП ВО)	Содержание компетенций согласно ФГОС (ОПОП ВО)	Индикаторы достижения компетенции согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
1	2	3	4
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке(ах)	Знать: правила устной и письменной коммуникации в целях взаимодействия в профессиональном сообществе Уметь: применять коммуникативные технологии в устной и письменной форме при решении академических и профессиональных задач Владеть: навыками профессионального взаимодействия в команде и с заинтересованными сторонами
ПК-5	Способность к установке, администрированию программных систем и систем управления базами данных, оптимизации функционирования информационных систем и баз данных; способность проводить анализ системных проблем обработки информации, разрабатывать предложения по реализации технического сопровождения и перспективного развития информационных систем и баз данных	ПК-5.1. Демонстрирует знание архитектуры и администрирования информационных систем, систем управления базами данных, системного программного обеспечения, требований информационной безопасности ПК-5.2. Демонстрирует умения выбирать аппаратное и программное обеспечение исходя из требований к	Знать: основные подходы к математической формализации различных аспектов безопасности информационных систем и реализации средств защиты информации этапы построения системы защиты информации, понятие политики безопасности; понятие информационных угроз и их виды, подходы к оценке информационных рисков; Уметь: настраивать основные средства обеспечения сетевой безопасности; разрабатывать

		функционированию ИС и баз данных, разрабатывать предложения по реализации сопровождения и развития информационных систем и ИТ-сервисов ПК-5.3. Имеет практический опыт установки, администрирования и интеграции программных систем и систем управления базами данных	программы для шифрования текста; применять математические методы и алгоритмы защиты информации Владеть: средствами защиты информации при решении профессиональных задач в области профессиональной деятельности

3. Содержание оценочных средств по дисциплине

3.1. Виды оценочных средств

Таблица 2. Виды оценочных средств.

№ п/п	Код компетенции/ планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1	УК-4.1. Обладает знаниями особенностей и правил личной и профессиональной устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) Знать: правила устной и письменной коммуникации в целях взаимодействия в профессиональном сообществе	Теория информации. Кодирование. Шифрование Информационная безопасность	Практическая работа	Задания теста № 1-146
2	УК-4.2. Демонстрирует умение применять современные коммуникативные технологии для академического и профессионального взаимодействия в ситуации устной и письменной коммуникации, в том числе на иностранном(ых) языке(ах) Уметь: применять коммуникативные технологии в устной и письменной форме при решении академических и профессиональных задач	Теория информации. Кодирование. Шифрование Информационная безопасность	Практическая работа	Задания теста № 35-56, 86-117, 138-146
3	УК-4.3. Имеет навыки академического и профессионального взаимодействия, в том числе на иностранном(ых) языке(ах) Владеть: навыками профессионального взаимодействия в команде и с заинтересованными сторонами	Теория информации. Кодирование. Шифрование Информационная безопасность	Практическая работа	Задания теста № 35-56, 86-117, 138-146
4	ПК-5.1. Демонстрирует знание архитектуры и администрирования	Теория информации. Кодирование. Шифрование	Практическая работа	Задания теста № 1-146

	информационных систем, систем управления базами данных, системного программного обеспечения, требований информационной безопасности Знать: основные подходы к математической формализации различных аспектов безопасности информационных систем и реализации средств защиты информации этапы построения системы защиты информации, понятие политики безопасности; понятие информационных угроз и их виды, подходы к оценке информационных рисков;	Информационная безопасность		
5	ПК-5.2. Демонстрирует умения выбирать аппаратное и программное обеспечение исходя из требований к функционированию ИС и баз данных, разрабатывать предложения по реализации сопровождения и развития информационных систем и ИТ-сервисов Уметь: настраивать основные средства обеспечения сетевой безопасности; разрабатывать программы для шифрования текста; применять математические методы и алгоритмы защиты информации	Теория информации. Кодирование. Шифрование Информационная безопасность	Практическая работа	Задания теста № 35-56, 86-117, 138-146
6	ПК-5.3. Имеет практический опыт установки, администрирования и интеграции программных систем и систем управления базами данных Владеть: средствами защиты информации при решении профессиональных задач в области профессиональной деятельности	Теория информации. Кодирование. Шифрование Информационная безопасность	Практическая работа	Задания теста № 35-56, 86-117, 138-146

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

3.2.Содержание оценочных средств

База тестовых вопросов

№ п/п	Формулировка вопроса	Варианты ответов (полужирным шрифтом – верные варианты)
1.	Что такое шифрование?	**a. способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого** b. совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств c. удобная среда для вычисления конечного пользователя
2.	Что такое кодирование?	**a. преобразование обычного, понятного текста в код** b. преобразование c. написание программы
3.	Сколько лет назад появилось шифрование?	**a. четыре тысячи лет назад** b. две тысячи лет назад c. пять тысяч лет назад
4.	Первое известное применение шифра:	**a. египетский текст** b. русский c. нет правильного ответа
5.	Секретная информация, которая хранится вWindows:	**a. пароли для доступа к сетевым ресурсам** **b. пароли для доступа в Интернет** **c. сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере**
6.	Что такое алфавит?	**a. конечное множество используемых для кодирования информации знаков** b. буквы текста

		c. нет правильного ответа
7.	Что такое текст?	**a. упорядоченный набор из элементов алфавита** b. конечное множество используемых для кодирования информации знаков c. все правильные
8.	Выберите примеры алфавитов:	**a. Z256 – символы, входящие в стандартные коды ASCII и КОИ-8** **b. восьмеричный и шестнадцатеричный алфавиты** c. AEE
9.	Что такое шифрование?	**a. преобразовательный процесс исходного текста в зашифрованный** b. упорядоченный набор из элементов алфавита c. нет правильного ответа
10.	Что такое дешифрование?	**a. на основе ключа шифрованный текст преобразуется в исходный** b. пароли для доступа к сетевым ресурсам c. сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере
11.	Что представляет собой криптографическая система?	**a. семейство T преобразований открытого текста, члены его семейства индексируются символом k** b. программу c. систему
12.	Что такое пространство ключей k?	**a. набор возможных значений ключа** b. длина ключа c. нет правильного ответа
13.	На какие виды подразделяют криптосистемы?	**a. симметричные** **b. ассиметричные** **c. с открытым ключом**
14.	Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:	**a. 1** b. 2 c. 3

15.	Количество используемых ключей в системах с открытым ключом:	**a. 2** b. 3 c. 1
16.	Ключи, используемые в системах с открытым ключом:	**a. открытый** **b. закрытый** c. нет правильного ответа
17.	Выберите то, как связаны ключи друг с другом в системе с открытым ключом:	**a. математически** b. логически c. алгоритмически
18.	Что принято называть электронной подписью?	**a. присоединяемое к тексту его криптографическое преобразование** b. текст c. зашифрованный текст
19.	Что такое криптостойкость?	**a. характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа** b. свойство гаммы c. все ответы верны
20.	Выберите то, что относится к показателям криптостойкости:	**a. количество всех возможных ключей** **b. среднее время, необходимое для криптоанализа** c. количество символов в ключе
21.	Требования, предъявляемые к современным криптографическим системам защиты информации:	**a. знание алгоритма шифрования не должно влиять на надежность защиты** **b. структурные элементы алгоритма шифрования должны быть неизменными** **c. не должно быть простых и легко устанавливаемых зависимостью между ключами** **+последовательно используемыми в процессе шифрования**
22.	Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:	**a. длина шифрованного текста должна быть равной лине исходного текста**

		b. зашифрованное сообщение должно поддаваться чтению только при наличии ключа c. нет правильного ответа
23.	Основными современными методами шифрования являются:	**a. алгоритм гаммирования** **b. алгоритмы сложных математических преобразований** **c. алгоритм перестановки**
24.	Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности?	**a. алгоритмом гаммирования** b. алгоритмом перестановки c. алгоритмом аналитических преобразований
25.	Чем являются символы оригинального текста, меняющиеся местами по определенному принципу, которые являются секретным ключом?	**a. алгоритм перестановки** b. алгоритм подстановки c. алгоритм гаммирования
26.	Самая простая разновидность подстановки:	**a. простая замена** b. перестановка c. простая перестановка
27.	Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера:	**a. 3** b. 4 c. 5
28.	Таблицы Вижинера, применяемые для повышения стойкости шифрования:	**a. во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке** **b. в качестве ключа используется случайность последовательных чисел** c. нет правильного ответа
29.	Суть метода перестановки:	**a. символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов** b. замена алфавита c. все правильные
30.	Цель криптоанализа:	**a. Определение стойкости алгоритма** b. Увеличение количества функций замещения в криптографическом алгоритме

		c. Уменьшение количества функций подстановок в криптографическом алгоритме d. Определение использованных перестановок
31.	По какой причине произойдет рост частоты применения брутфорс-атак?	a. Возросло используемое в алгоритмах количество перестановок и замещений b. Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам **c. Мощность и скорость работы процессоров возросла** d. Длина ключа со временем уменьшилась
32.	Не будет являться свойством или характеристикой односторонней функции хэширования:	a. Она преобразует сообщение произвольной длины в значение фиксированной длины b. Имея значение дайджеста сообщения, невозможно получить само сообщение c. Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко **d. Она преобразует сообщение фиксированной длины в значение переменной длины**
33.	Выберите то, что указывает на изменение сообщения:	a. Изменился открытый ключ b. Изменился закрытый ключ **c. Изменился дайджест сообщения** d. Сообщение было правильно зашифровано
34.	Алгоритм американского правительства, который предназначен для создания безопасных дайджестов сообщений:	a. Data Encryption Algorithm b. Digital Signature Standard **c. Secure Hash Algorithm** d. Data Signature Algorithm
35.	Выберите то, что лучшеописывает отличия между HMAC и CBC-MAC?	a. HMAC создает дайджест сообщения и применяется для контроля целостности;

		CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности b. HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы **c. HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC** d. HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком
36.	Определите преимущество RSA над DSA?	**a. Он может обеспечить функциональность цифровой подписи и шифрования** b. Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи c. Это блочный шифр и он лучше поточного d. Он использует одноразовые шифровальные блокноты
37.	С какой целью многими странами происходит ограничение использования и экспорта криптографических систем?	a. Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах b. Эти системы могут использоваться некоторыми странами против их местного населения **c. Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования**

		d. Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему
38.	Выберите то, что используют для создания цифровой подписи:	a. Закрытый ключ получателя b. Открытый ключ отправителя **c. Закрытый ключ отправителя** d. Открытый ключ получателя
39.	Выберите то, что лучше всего описывает цифровую подпись:	a. Это метод переноса собственноручной подписи на электронный документ b. Это метод шифрования конфиденциальной информации c. Это метод, обеспечивающий электронную подпись и шифрование **d. Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения**
40.	Эффективная длина ключа в DES:	**a. 56** b. 64 c. 32 d. 16
41.	Причина, по которой удостоверяющий центр отзывает сертификат:	a. Если открытый ключ пользователя скомпрометирован b. Если пользователь переходит на использование модели PEM, которая использует сеть доверия **c. Если закрытый ключ пользователя скомпрометирован** d. Если пользователь переходит работать в другой офис
42.	Выберите то, что лучше всего описывает удостоверяющий центр?	a. Организация, которая выпускает закрытые ключи и соответствующие алгоритмы b. Организация, которая проверяет процессы

		шифрования c. Организация, которая проверяет ключи шифрования **d. Организация, которая выпускает сертификаты**
43.	Расшифруйте аббревиатуру DEA:	a. Data Encoding Algorithm b. Data Encoding Application **c. Data Encryption Algorithm** d. Digital Encryption Algorithm
44.	Разработчик первого алгоритма с открытыми ключами:	a. Ади Шамир b. Росс Андерсон c. Брюс Шнайер **d. Мартин Хеллман**
45.	Процесс, выполняемый после создания сеансового ключа DES:	a. Подписание ключа b. Передача ключа на хранение третьей стороне (key escrow) c. Кластеризация ключа **d. Обмен ключом**
46.	Количество циклов перестановки и замещения, выполняемый DES:	**a. 16** b. 32 c. 64 d. 56
47.	Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:	a. Оно обеспечивает проверку целостности и правильности данных **b. Оно требует внимательного отношения к процессу управления ключами** c. Оно не требует большого количества системных ресурсов d. Оно требует передачи ключа на хранение третьей стороне (escrowed)
48.	Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:	a. Коллизия b. Хэширование c. MAC **d. Кластеризация ключей**
49.	Определение фактора трудозатрат для алгоритма:	a. Время зашифрования и расшифрования открытого текста **b. Время, которое займет взлом шифрования** c. Время, которое занимает

		выполнение 16 циклов преобразований d. Время, которое занимает выполнение функций подстановки
50.	Основная цельиспользования одностороннего хэширования пароля пользователя:	a. Это снижает требуемый объем дискового пространства для хранения пароля пользователя **b. Это предотвращает ознакомление кого-либо с открытым текстом пароля** c. Это позволяет избежать избыточной обработки, требуемой асимметричным алгоритмом d. Это предотвращает атаки повтора (replay attack)
51.	Алгоритм, основанный на сложности разложения больших чисел на два исходных простых сомножителя:	a. ECC **b. RSA** c. DES d. Диффи-Хеллман
52.	Что является описанием разницы алгоритмов DES и RSA:	**a. DES – это симметричный алгоритм, а RSA – асимметричный** b. DES – это асимметричный алгоритм, а RSA – симметричный c. Они оба являются алгоритмами хэширования, но RSA генерирует 160-битные значения хэша d. DES генерирует открытый и закрытый ключи, а RSA выполняет шифрование сообщений
53.	Алгоритм, использующий симметричный ключ и алгоритм хэширования:	**a. HMAC** b. 3DES c. ISAKMP-OAKLEY d. RSA
54.	Количество способов гаммирования:	**a. 2** b. 5 c. 3
55.	Показатель стойкости шифрования методом гаммирования:	**a. свойство гаммы** b. длина ключа c. нет правильного ответа
56.	То, что применяют в качестве гаммы:	**a. любая последовательность случайных символов**

		b. число c. все ответы верны
57.	Метод, который применяют при шифровании с помощью аналитических преобразований:	**a. алгебры матриц** b. матрица c. факториал
58.	То, что применяют в качестве ключа при шифровании с помощью аналитических преобразований:	**a. матрица A** b. вектор c. обратная матрица
59.	Способ осуществления дешифрования текста при аналитических преобразованиях:	**a. умножение матрицы на вектор** b. деление матрицы на вектор c. перемножение матриц
60.	Как называют комплекс (аппаратура и программное обеспечение), который по результатам анализа контролируемых и собираемых данных принимает решение о наличии атаки или вторжения?	**a. система обнаружения вторжений** b. межсетевой экран c. антивирусное средство d. средства контроля доступа и аутентификации
61.	Какие системы обнаружения вторжений осуществляют анализ активности отдельного компьютера?	a. сетевые **b. хостовые** c. гибридные d. мобильные
62.	Какие системы обнаружения вторжений выполняют функции хостовых систем обнаружения вторжений и при этом используют и анализ сетевых пакетов, приходящих на данный хост?	a. сетевые b. хостовые **c. гибридные** d. мобильные
63.	На какие системы обнаружения атак подразделяются по структуре?	**a. централизованные** **b. децентрализованные** c. демилитаризованные d. иерархические
64.	Какие различают системы обнаружения вторжений по характеру реакции?	**a. активные** **b. пассивные** c. перманентные d. незамедлительные
65.	Какие подходы могут использоваться для обнаружения сигнатур?	**a. Совпадение с шаблоном** **b. Совпадение с шаблоном состояния** **c. Анализ на основе шаблона используемого протокола** **d. Эвристический подход**
66.	В каком случае обнаружение сигнатур базируется на поиске фиксированной последовательности байтов в рассматриваемом элементе данных (например, в единичном пакете)?	**a. Совпадение с шаблоном** b. Совпадение с шаблоном состояния

		c. Анализ на основе шаблона используемого протокола d. Эвристический подход
67.	В каком случае обнаружение сигнатур происходит следующим образом: по одному пакету устанавливается состояние потока данных, появление другого пакета (или пакетов), который соответствует данным состояния, считается атакой?	a. Совпадение с шаблоном **b. Совпадение с шаблоном состояния** c. Анализ на основе шаблона используемого протокола d. Эвристический подход
68.	В каком случае обнаружение сигнатур происходит таким образом, что для формирования состояния используется декодирование различных элементов протокола? В этом случае при декодировании протокола СОВ применяет правила, определенные RFC для нарушений. В некоторых случаях эти нарушения могут находиться в определенных полях протокола, что требует более детального анализа.	a. Совпадение с шаблоном b. Совпадение с шаблоном состояния **c. Анализ на основе шаблона используемого протокола** d. Эвристический подход
69.	Какой подход обнаружения сигнатур использует логические правила, полученные эвристически?	a. Совпадение с шаблоном b. Совпадение с шаблоном состояния c. Анализ на основе шаблона используемого протокола **d. Эвристический подход**
70.	Какие различают виды сигнатур?	**a. Сигнатуры эксплойта** **b. Сигнатуры уязвимости** **c. Сигнатуры аномалий протоколов** d. Сигнатуры анамалий
71.	действия, предпринимаемые злоумышленником, против компьютера (или сети) потенциальной жертвы, это?	**a. атака** b. вторжение c. угроза d. уязвимость
72.	Какие сигнатуры опираются на характеристики атаки, которые позволяют однозначно идентифицировать атаку?	**a. Сигнатуры эксплойта** b. Сигнатуры уязвимости c. Сигнатуры аномалий протоколов
73.	Какие сигнатуры опираются на особенности конкретной уязвимости, т.е. на те параметры или действия, которые необходимо выполнить для использования данной уязвимости?	a. Сигнатуры эксплойта **b. Сигнатуры уязвимости** c. Сигнатуры аномалий протоколов
74.	Какие сигнатуры иногда трактуются как обнаружение аномалий протокола? Для разработки таких сигнатур необходимо провести анализ реализации рассматриваемого протокола на соответствие RFC.	a. Сигнатуры эксплойта b. Сигнатуры уязвимости **c. Сигнатуры аномалий протоколов**

75.	Некоторые современные СОВ нельзя отнести ни к системам обнаружения сигнатур, ни к системам обнаружения аномалий. Они опираются на новые (иногда их называют альтернативные) подходы к обнаружению. Какие подходы можно отнести к числу альтернативных подходов?	**a. методы Data Mining** **b. методы технологии мобильных агентов** **c. методы построения иммунных систем** **d. применение генетических алгоритмов** **e. применение нейронных сетей** f. методы нейролингвистического программирования
76.	Какую технологию можно определить как процесс обнаружения в необработанных данных: - ранее неизвестных; - нетривиальных; - практически полезных; - доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности?	**a. технология Data Mining** b. технология мобильных агентов c. методы построения иммунных систем d. применение генетических алгоритмов e. применение нейронных сетей
77.	Каковы основные методы обхода сетевых систем обнаружения вторжений?	**a. сбивание с толку** **b. фрагментация** **c. шифрование** **d. перегрузка** e. социальная инженерия
78.	Какой метод обхода сетевых систем обнаружения вторжений заключается в манипулировании данными таким образом, чтобы сигнатура СОВ не соответствовала проходящему пакету, который бы интерпретировался приемной стороной (например, посылка пакета, использующего кодирование, или добавление вспомогательных символов)?	**a. сбивание с толку** b. фрагментация c. шифрование d. перегрузка
79.	Какой метод обхода сетевых систем обнаружения вторжений заключается в разбивке пакета данных на фрагменты, которые можно послать в различном порядке (и с различными временными интервалами между ними)?	a. сбивание с толку **b. фрагментация** c. шифрование d. перегрузка
80.	Какой метод обхода сетевых систем обнаружения вторжений заключается в действиях нарушителя с целью противодействовать сетевым системам обнаружения атак исследовать полезную нагрузку пакета?	a. сбивание с толку b. фрагментация **c. шифрование** d. перегрузка
81.	Какой метод обхода сетевых систем обнаружения вторжений заключается в переполнении сетевой системы обнаружения вторжений?	a. сбивание с толку b. фрагментация c. шифрование **d. перегрузка**
82.	Несанкционированный вход в информационную систему (в результате действий, нарушающих политику безопасности или обходящих систему защиты), это?	**a. вторжение** b. атака c. угроза d. уязвимость

83.	Для хостовых систем обнаружения вторжений обычно используется комбинация обнаружения аномалий и обнаружения сигнатур. Одним из основных для хостовых СОВ является вопрос: если хост будет скомпрометирован, то как удержать нарушителя от манипулирования с элементами СОВ для предотвращения обнаружения атаки? Какие методы для этого являются основными?	**a. контроль расположения и целостности файлов** **b. сбивание с толку** **c. вставка нулевого знака в запрос после указания метода** **d. перехват приложения** e. социальная инженерия
84.	Как называют генерацию сигнала об обнаружении атаки (вторжения), которой не было?	**a. ложная тревога** b. пропуск c. атака d. вторжение
85.	Как называют пропуск атаки или вторжения (отсутствие сигнала тревоги при наличии вторжения)?	**a. пропуск** b. ложная тревога c. уязвимость d. вторжение
86.	Для построения таксономии систем обнаружения атак необходимо выбрать критерии, согласно которым будет проводиться классификация. Один из подходов выбора критериев – это подход, в котором в качестве таких критериев выбраны типичные функции и особенности проектирования и реализации систем обнаружения атак. Какие это функции?	**a. подход к обнаружению** **b. защищаемая система** **c. структура СОВ** **d. источник данных (для принятия решения)** **e. время анализа** **f. характер реакции** g. блокировка трафика
87.	Какие выделяют подходы к обнаружению атак?	**a. обнаружение сигнатур** **b. обнаружение аномалий** **c. гибридный подход** d. обнаружение вторжений
88.	Какие выделяют виды систем обнаружения атак?	**a. хостовые** **b. сетевые** **c. гибридные** d. мобильные
89.	Какие системы обнаружения вторжений осуществляют сбор и анализ сетевых пакетов, на основании которых проводится обнаружение?	**a. сетевые** b. хостовые c. гибридные d. мобильные
90.	Как называют сеть на уровне компании, в которой используются программные средства, основанные на стеке протоколов TCP/IP?	**a. Корпоративная сеть (интранет)** b. Экстранет-сеть c. Полно-связная сеть d. Глобальная сеть
91.	Негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде, это?	a. Отказ b. Сбой c. Ошибка **d. Побочное влияние**
92.	Какое происхождение угрозы обусловливается злоумышленными	a. случайное

	действиями людей, осуществляемыми в целях реализации одного или нескольких видов угроз?	**b. преднамеренное** c. субъективное d. объективное
93.	Какие выделяют разновидности предпосылок появления угроз?	a. случайные b. преднамеренные **c. субъективные** **d. объективные**
94.	Отмечают две разновидности предпосылок появления угроз: объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведывательных служб иностранных государств, промышленный шпионаж, деятельность криминальных и хулиганствующих элементов, злоумышленные действия недобросовестных сотрудников системы). Перечисленные разновидности предпосылок интерпретируются разным образом. Как называют следующую интерпретацию: Физическая нехватка одного или нескольких элементов системы обработки данных, вызывающая нарушения технологического процесса обработки и (или) перегрузку имеющихся элементов.	**a. количественная недостаточность** b. качественная недостаточность c. деятельность разведывательных служб иностранных государств d. промышленный шпионаж e. действия криминальных и хулиганствующих элементов f. злоумышленные действия недобросовестных сотрудников
95.	Отмечают две разновидности предпосылок появления угроз: объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведывательных служб иностранных государств, промышленный шпионаж, деятельность криминальных и хулиганствующих элементов, злоумышленные действия недобросовестных сотрудников системы). Перечисленные разновидности предпосылок интерпретируются разным образом. Как называют следующую интерпретацию: Несовершенство конструкции (организации) элементов системы, в силу чего могут появляться возможности для случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию.	a. количественная недостаточность **b. качественная недостаточность** c. деятельность разведывательных служб иностранных государств d. промышленный шпионаж e. действия криминальных и хулиганствующих элементов f. злоумышленные действия недобросовестных сотрудников
96.	Отмечают две разновидности предпосылок появления угроз: объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведывательных служб иностранных государств, промышленный шпионаж, деятельность криминальных и хулиганствующих элементов, злоумышленные действия недобросовестных сотрудников системы). Перечисленные разновидности предпосылок интерпретируются разным образом. Как называют следующую интерпретацию: Специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами.	a. количественная недостаточность b. качественная недостаточность **c. деятельность разведывательных служб иностранных государств** d. промышленный шпионаж e. действия криминальных и хулиганствующих элементов f. злоумышленные действия недобросовестных сотрудников
97.	Отмечают две разновидности предпосылок появления угроз: объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведывательных служб иностранных государств, промышленный шпионаж, деятельность криминальных и	a. количественная недостаточность b. качественная недостаточность c. деятельность

	хулиганствующих элементов, злоумышленные действия недобросовестных сотрудников системы). Перечисленные разновидности предпосылок интерпретируются разным образом. Как называют следующую интерпретацию: Негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной ее утечки или похищения, а также по созданию для себя благоприятных условий в целях получения максимальной выгоды.	разведывательных служб иностранных государств **d. промышленный шпионаж** e. действия криминальных и хулиганствующих элементов f. злоумышленные действия недобросовестных сотрудников
98.	Отмечают две разновидности предпосылок появления угроз: объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведывательных служб иностранных государств, промышленный шпионаж, деятельность криминальных и хулиганствующих элементов, злоумышленные действия недобросовестных сотрудников системы). Перечисленные разновидности предпосылок интерпретируются разным образом. Как называют следующую интерпретацию: Хищение информации или компьютерных программ в целях наживы или их разрушение в интересах конкурентов.	a. количественная недостаточность b. качественная недостаточность c. деятельность разведывательных служб иностранных государств d. промышленный шпионаж **e. действия криминальных и хулиганствующих элементов** f. злоумышленные действия недобросовестных сотрудников
99.	Отмечают две разновидности предпосылок появления угроз: объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведывательных служб иностранных государств, промышленный шпионаж, деятельность криминальных и хулиганствующих элементов, злоумышленные действия недобросовестных сотрудников системы). Перечисленные разновидности предпосылок интерпретируются разным образом. Как называют следующую интерпретацию: Хищение (копирование) или уничтожение информационных массивов и (или) программ по эгоистическим или корыстным мотивам.	a. количественная недостаточность b. качественная недостаточность c. деятельность разведывательных служб иностранных государств d. промышленный шпионаж e. действия криминальных и хулиганствующих элементов **f. злоумышленные действия недобросовестных сотрудников**
100.	Какие принципы информационной гарантированности рекомендует стратегия эшелонированной обороны:	**a. применение защиты во множественных местах. Поскольку злоумышленники могут атаковать систему из множества мест, включая внешние и внутренние, организация должна применять защитные механизмы в различных точках, которые должны обеспечивать защиту сетей и инфраструктуры, защиту границ сети и территории, а также защиту компьютерного**

		оборудования; **b. применение уровневой защиты предполагает установку защитных механизмов между потенциальным злоумышленником и целью;** **c. определение устойчивости безопасности достигается оценкой защитных возможностей каждого компонента информационной гарантированности;** **d. применение инфраструктуры обнаружения атак и вторжений, использование методов и средств анализа и корреляции получаемых данной инфраструктурой результатов.**
101.	Как называют интранет-сеть, подключенную к Интернету, т.е. сеть типа интранет, но санкциони-рующая доступ к ее ресурсам определенной категории пользователей, наделенной соответствующими полномочиями?	**a. Экстранет-сеть** b. Глобальная сеть c. Индивидуальная сеть d. Корпоративная сеть
102.	Что из нижеперечисленного является источником угроз?	**a. люди** **b. технические средства** **c. модели, алгоритмы и программы** **d. технологические схемы обработки данных** **e. внешняя среда** f. инопланетный разум
103.	Рассматривая источники угроз, как определяют группу источников попадающих под следующее описание: персонал, пользователи и посторонние лица, которые могут взаимодействовать с ресурсами и данными организации непосредственно с рабочих мест и удаленно, используя сетевое взаимодействие.	**a. люди** b. технические средства c. модели, алгоритмы и программы d. технологические схемы обработки данных e. внешняя среда
104.	Рассматривая источники угроз, как определяют группу источников попадающих под следующее описание: непосредственно связанные с обработкой, хранением и передачей информации (например, средства регистрации данных, средства ввода и т.д.), и вспомогательные (например, средства электропитания, кондиционирования и т.д.).	a. люди **b. технические средства** c. модели, алгоритмы и программы d. технологические схемы обработки данных e. внешняя среда
105.	Рассматривая источники угроз, как определяют группу источников попадающих под следующее описание: эту группу	a. люди b. технические средства

	источников рассматривают как недостатки проектирования, реализации и конфигурации (эксплуатации).	**c. модели, алгоритмы и программы** d. технологические схемы обработки данных e. внешняя среда
106.	Рассматривая источники угроз, как определяют группу источников попадающих под следующее описание: выделяют ручные, интерактивные, внутримашинные и сетевые технологические схемы обработки.	a. люди b. технические средства c. модели, алгоритмы и программы **d. технологические схемы обработки данных** e. внешняя среда
107.	Рассматривая источники угроз, как определяют группу источников попадающих под следующее описание: выделяют состояние среды (возможность пожаров, землетрясений и т.п.), побочные шумы (особенно опа-сные при передаче данных) и побочные сигналы (например, электромагнитное излучение аппаратуры).	a. люди b. технические средства c. модели, алгоритмы и программы d. технологические схемы обработки данных **e. внешняя среда**
108.	Перечислите основные причины утечки информации.	**a. несоблюдение персоналом норм, требований, правил эксплуатации** **b. ошибки в проектировании системы и систем защиты** **c. ведение противостоящей стороной технической и агентурной разведок**
109.	Какие виды утечки выделяют в соответствии с ГОСТ 50922-96?	**a. разглашение** **b. несанкционированный доступ к информации** **c. получение защищаемой информации разведками**
110.	Что понимается под несанкционированным доведением защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации?	**a. Разглашение информации** b. Несанкционированный доступ к информации c. Получение защищаемой информации разведками
111.	Что понимается под получением защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации?	**a. Несанкционированный доступ** b. Разглашение информации c. Получение защищаемой информации разведками
112.	Какие можно выделить особенности корпоративных сетей, которые представляют повышенную опасность для выполнения ими своих функциональных задач?	**a. глобальность связей** **b. масштабность** **c. гетерогенность** d. изолированность

113.	С помощью чего может осуществляться получение защищаемой информации разведками?	**a. технические средства** **b. агентурные методы** c. воздушные средства d. методы глубокого анализа
114.	Что называют совокупностью источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя?	**a. канал утечки информации** b. информационный канал c. уязвимый канал
115.	Что понимается под «информационной безопасностью»?	**a. Защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.** b. Искусство и наука использования всех элементов государства в мирное и военное время для обеспечения защиты национальных интересов. c. Наука о комфортном и травмобезопасном взаимодействии человека со средой обитания. d. Состояние защищённости жизненно-важных интересов личности, общества, организации, предприятия от потенциально и реально существующих угроз, или отсутствие таких угроз.
116.	На каких уровнях должны применяться меры обеспечения безопасности?	**a. законодательный** **b. административный** **c. процедурный** **d. программно-технический** e. бытовой
117.	Какие этапы должны включать в себя работы по обеспечению режима информационной безопасности организации?	**a. определение политики ИБ (Документы политики безопасности)** **b. определение сферы**

		(границ) системы управления информационной безопасностью и конкретизация целей ее создания (Документы, определяющие границы системы) **c. оценка рисков (Описание угроз, уязвимостей и оценка возможного ущерба)** **d. управление рисками** **e. выбор контрмер, обеспечивающих режим ИБ (Выбор контрмер для каждого из уровней, Построение комплексной системы обеспечения ИБ)** **f. аудит системы управления ИБ**
118.	Назовите основные свойства безопасности?	**a. конфиденциальность** **b. целостность** **c. доступность** d. постоянность e. равномерность f. непрерывность
119.	Свойство безопасности при котором информация доступна только тем, кто авторизован для доступа?	**a. конфиденциальность** b. целостность c. доступность d. неотказуемость e. подотчётность f. достоверность g. аутентичность
120.	Свойство безопасности при котором гарантирована точность, полнота и методы обработки информации?	**a. целостность** b. конфиденциальность c. доступность d. неотказуемость e. подотчётность f. достоверность g. аутентичность
121.	Свойство безопасности при котором информация и ассоциированные объекты доступны по требованию авторизованных пользователей?	**a. доступность** b. конфиденциальность c. целостность d. неотказуемость e. подотчётность f. достоверность g. аутентичность
122.	Что называют планом высокого уровня, в котором описываются цели и задачи организации, а также мероприятия в сфере обеспечения безопасности?	**a. Политика информационной безопасности**

		b. Модель угроз c. Положение о конфиденциальной информации d. Концепция безопасности
123.	Как называют любую характеристику, использование которой нарушителем может привести к реализации угрозы?	**a. уязвимость информационной системы** b. угроза информационной системе c. риск безопасности информационной системы
124.	Какие разделы может включать в себя реальная политика безопасности организации?	**a. общие положения** **b. политика управления паролями** **c. идентификация пользователей** **d. полномочия пользователей** **e. защита информационных ресурсов организации от компьютерных вирусов** **f. правила установки и контроля сетевых соединений** **g. правила политики безопасности по работе с системой электронной почты** **h. правила обеспечения безопасности информационных ресурсов** **i. обязанности пользователей по выполнению правил политики безопасности**
125.	Какие типы сетевых периметров можно выделить?	**a. внешний** **b. внутренний** c. кольцевой d. федеральный
126.	Какой сетевой периметр идентифицирует точку разделения между устройствами, которые контролируются, и теми, которые не контролируются?	**a. Внешний сетевой периметр** b. Внутренний сетевой периметр c. Территориальный сетевой периметр d. Иерархический сетевой периметр
127.	Какой тип сетевого периметра представляет собой дополнительные границы, в которых размещаются другие механизмы безопасности, такие как МЭ и фильтрующие	**a. Внутренний сетевой периметр** b. Внешний сетевой

	маршрутизаторы?	периметр c. Территориальный сетевой периметр d. Иерархический сетевой периметр
128.	Как называют сети внутри сетевого периметра, над которыми специалисты организации имеют полный административный контроль?	**a. доверенные сети** b. недоверенные сети c. демилитаризованная зона d. эшелонированные сети
129.	Как называются сети, которые находятся вне установленного сетевого периметра и находящиеся вне контроля?	**a. недоверенные сети** b. доверенные сети c. демилитаризованная зона d. эшелонированные сети
130.	Как называется область внешнего периметра в которой серверы, отвечающие на запросы из внешней сети, ограничены в доступе к основным сегментам внутреннего периметра сети, с целью минимизировать ущерб, при взломе одного из общедоступных сервисов?	**a. демилитаризованная зона** b. недоверенная сеть c. доверенная сеть d. эшелонированная сеть
131.	Что понимается под практической стратегией достижения информационной гарантированности в сетевом оборудовании? (эта стратегия представляет собой баланс между свойствами защиты и стоимостью, производительностью и функциональными характеристиками)	**a. Эшелонированная оборона** b. Территориальная оборона c. Государственная оборона d. Вражеская оборона
132.	Как называют потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба (материального, морального или иного) ресурсам системы?	**a. угроза информационной системе** b. уязвимость информационной системы c. риск безопасности информационной системы
133.	Какое происхождение угроз обуславливается спонтанными и не зависящими от воли людей обстоятельствами, возникающими в системе обработки данных в процессе ее функционирования?	**a. случайное** b. преднамеренное c. субъективное d. объективное
134.	Нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им основных своих функций, это?	**a. Отказ** b. Сбой c. Ошибка d. Побочное влияние
135.	Временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции, это?	a. Отказ **b. Сбой** c. Ошибка d. Побочное влияние
136.	Неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния, это?	a. Отказ b. Сбой **c. Ошибка** d. Побочное влияние

137.	Что организация ценит и хочет защитить?	**a. Ресурсы** b. Честь c. Уязвимости d. Контроль безопасности
138.	В процессе идентификации уязвимостей, какие могут применяться документированные источники данных по уязвимостям?	**a. результаты предыдущих оценок риска** **b. отчеты аудита ИТ системы, отчеты о системных аномалиях, отчеты с обзорами безопасности, отчеты системных тестах и оценках** **c. списки уязвимостей, например, из баз данных уязвимостей** **d. информационные бюллетени по безопасности** **e. информационные бюллетени изготовителей** **f. коммерческие компании, выполняющие функции информационного аудита безопасности** **g. анализ безопасности системного ПО** **h. тестирование системной безопасности** i. литература
139.	Для оценки реального наличия уязвимостей могут применяться методы тестирования (включая системное тестирование) для идентификации системных уязвимостей в зависимости от критичности ИТ системы и доступных ресурсов. Что включают в себя методы тестирования?	**a. средства автоматического сканирования уязвимостей** **b. тесты и оценка безопасности** **c. тесты на проникновение** d. средства удаленного администрирования
140.	Что используется для сканирования групп хостов или сети на известные уязвимые службы? Необходимо заметить, что некоторые потенциальные уязвимости, определенные таким автоматическим средством, могут не представлять реальных уязвимостей в контексте реального системного оборудования организации.	**a. средства автоматического сканирования уязвимостей** b. тесты и оценка безопасности c. тесты на проникновение
141.	Что может быть использовано для идентификации уязвимостей во время процесса оценки риска?	a. средства автоматического сканирования уязвимостей **b. тесты и оценка безопасности** c. тесты на проникновение
142.	Что может использоваться для оценки контроля безопасности и уверенности в том, что различные аспекты ИТ системы	a. средства автоматического сканирования уязвимостей

	защищены?	b. тесты и оценка безопасности **c. тесты на проникновение**
143.	Целью какого шага оценки риска является анализ применяемых или планируемых к применению средств защиты (контроля) в организации для минимизации или устранения вероятности уязвимости, реализуемой источником угроз?	a. характеристика системы b. идентификация угроз c. идентификация уязвимостей **d. анализ средств защиты (контроля)** e. определение вероятностей (ранжирование частот появления) f. анализ влияния g. определение риска h. рекомендации по средствам защиты (контролю) i. результирующая документация
144.	Цель какого шага оценки риска состоит в определении нежелательного влияния успешной реализа-ции уязвимостей угрозами?	a. характеристика системы b. идентификация угроз c. идентификация уязвимостей d. анализ средств защиты (контроля) e. определение вероятностей (ранжирование частот появления) **f. анализ влияния** g. определение риска h. рекомендации по средствам защиты (контролю) i. результирующая документация
145.	При проведении анализа влияния цель состоит в определении нежелательного влияния успешной реализации уязвимостей угрозами. Какую информацию необходимо получить для этого?	**a. миссия системы (т.е. процессы, осуществляемые ИТ системой)** **b. критичность системы и данных (т.е. значение или важность системы для организации)** **c. чувствительность системы и данных** d. информация об аналогичных системах
146.	Назначением какого шага оценки риска является оценка уровня риска ИТ системы?	a. характеристика системы b. идентификация угроз c. идентификация уязвимостей d. анализ средств защиты

		(контроля) e. определение вероятностей (ранжирование частот появления) f. анализ влияния **g. определение риска** h. рекомендации по средствам защиты (контролю) i. результирующая документация

4. Порядок проведения и критерии оценивания промежуточной аттестации

4.1. Порядок проведения промежуточной аттестации

Зачёт проводится в виде тестирования. Студент должен ответить на вопросы закрытого типа, которые предполагают выбор вариантов ответа. Всего 20 тестовых вопросов. Продолжительность теста – 35 минут.

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

Тест формируется в системе электронного обучения MOODLE.
Максимальный балл за тест — 100 баллов.

Оценка	Зачтено	Незачтено
Баллы	100-60 баллов	59-0 баллов
Уровень освоения проверяемых компетенций	высокий	низкий

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

Для получения зачета обучающийся должен выполнить все практические работы.

0-59 баллов – незачет;
60-100 баллов – зачет;

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

Уровни сформированности компетенций определяется следующим образом:

1. Высокий уровень сформированности компетенций соответствует оценке зачтено:

- предполагает формирование компетенций на высоком уровне;
- знание теоретических разделов изучаемой дисциплины на уровне не ниже оценки удовлетворительно;
- студент умеет применять на практике знания, полученные в рамках изучения дисциплины
- формируются навыки использования теоретических и практических разделов дисциплины для решения задач профессиональной деятельности;

2. Низкий уровень соответствует оценке незачтено.