Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю)
«Защита информации»

Направление подготовки (специальность)
09.03.04 «Программная инженерия»

Направленность (профиль)
«Информационные системы и интеллектуальные технологии»

Присваиваемая квалификация
Бакалавр

Форма обучения
Очная

Год набора
2025

Челябинск, 2025 г.

09.03.04 Программная инженерия, Информационные системы и интеллектуальные технологии, бакалавр, *Защита информации*, 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: 09.03.04 Программная инженерия
Направленность: Информационные системы и интеллектуальные технологии
Дисциплина: Защита информации
Семестр: 7
Форма промежуточной аттестации: экзамен
Для оценивания результатов обучения используется балльно-рейтинговая система.

2. Перечень формируемых компетенций

Изучение дисциплины «Защита информации» 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 осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.1 Имеет представление о правилах и принципах деловой устной и письменной коммуникации на государственном языке Российской Федерации и иностранном(ых) языке(ах) УК-4.2 Демонстрирует умение осуществлять деловую коммуникацию в устной и письменной формах, использовать методы и навыки делового общения УК-4.3 Имеет навыки делового общения на государственном языке Российской Федерации и иностранном(ых) языке(ах)	Знать:понятие информационных угроз и их виды, подходы к оценке информационных рисков; основные принципы функционирования сетей и методы обеспечения их безопасности; требования к подготовке презентаций, оформлению научно-технических отчетов. Уметь:применять методы оценки рисков информационной безопасности, применять компьютер для производства работ в области защиты информации; настраивать основные средства обеспечения сетевой безопасности; представлять результаты работы в виде статей и докладов. Владеть:Навыками описания выявленных уязвимостей и рекомендаций по их устранению
ПК-1	Владение навыками использования операционных систем, сетевых технологий, современных языков программирования, технологий обработки данных, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных	ПК-1.1. Демонстрирует знание основ операционных систем, сетевых технологий, языков программирования, баз данных и технологий обработки данных, основ проектирования интерфейсов, языков и методов формальных спецификаций ПК-1.2. Демонстрирует умения разрабатывать системное и прикладное программного обеспечение с использованием языков и технологий программирования, баз данных, сетевых	Знать:этапы построения системы защиты информации, понятие политики безопасности. Уметь:применять основные методы и средства обеспечения безопасности. Владеть:навыками настройки безопасности в Windows системе.

		технологий и операционных систем, языков и методов формальных спецификаций ПК-1.3. Имеет практический опыт использования операционных систем, современных языков программирования, систем управления базами данных и технологий обработки данных, средств разработки программного интерфейса	

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 Имеет представление о правилах и принципах деловой устной и письменной коммуникации на государственном языке Российской Федерации и иностранном(ых) языке(ах) Знать:понятие информационных угроз и их виды, подходы к оценке информационных рисков; основные принципы функционирования сетей и методы обеспечения их безопасности; требования к подготовке презентаций, оформлению научно-технических отчетов.	Введение в теорию множеств математическую логику Элементы комбинаторики. Введение в теорию графов. Кольца. Поля. Группы	Тест, собеседование, проверка практических работ	Задания теста № 1-106 Задания теста № 107-187
2	УК-4.2 Демонстрирует умение осуществлять деловую коммуникацию в устной и письменной формах, использовать методы и навыки делового общения Уметь:применять методы оценки рисков информационной безопасности, применять компьютер для производства работ в области защиты информации; настраивать основные средства обеспечения сетевой безопасности; представлять результаты работы в виде статей и докладов.	Введение в теорию множеств математическую логику Элементы комбинаторики. Введение в теорию графов. Кольца. Поля. Группы	Тест, собеседование, проверка практических работ	Задания теста № 1-106 Задания теста № 107-187
3	УК-4.3 Имеет навыки делового общения на государственном языке Российской Федерации и иностранном(ых) языке(ах) Владеть:Навыками описания выявленных уязвимостей и рекомендаций по их устранению	Введение в теорию множеств математическую логику Элементы комбинаторики. Введение в теорию графов. Кольца. Поля. Группы	Тест, собеседование, проверка практических работ	Задания теста № 1-106 Задания теста № 107-187

4	ПК-1.1. Демонстрирует знание основ операционных систем, сетевых технологий, языков программирования, баз данных и технологий обработки данных, основ проектирования интерфейсов, языков и методов формальных спецификаций Знать:этапы построения системы защиты информации, понятие политики безопасности.	Введение в теорию множеств математическую логику Элементы комбинаторики. Введение в теорию графов. Кольца. Поля. Группы	Тест, собеседование, проверка практических работ	Задания теста № 1-106 Задания теста № 107-187
5	ПК-1.2. Демонстрирует умения разрабатывать системное и прикладное программного обеспечение с использованием языков и технологий программирования, баз данных, сетевых технологий и операционных систем, языков и методов формальных спецификаций Уметь:применять основные методы и средства обеспечения безопасности.	Введение в теорию множеств математическую логику Элементы комбинаторики. Введение в теорию графов. Кольца. Поля. Группы	Тест, собеседование, проверка практических работ	Задания теста № 1-106 Задания теста № 107-187
6	ПК-1.3. Имеет практический опыт использования операционных систем, современных языков программирования, систем управления базами данных и технологий обработки данных, средств разработки программного интерфейса Владеть:навыками настройки безопасности в Windows системе.	Введение в теорию множеств математическую логику Элементы комбинаторики. Введение в теорию графов. Кольца. Поля. Группы	Тест, собеседование, проверка практических работ	Задания теста № 1-106 Задания теста № 107-187

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

В процессе прохождения текущей аттестации студенты должны выполнить практические работы и написать отчет по ним. Часть материала студентам выдается на английском языке.

База тестовых вопросов

№ п/п	Формулировка вопроса	Варианты ответов (полужирным шрифтом – верные варианты)
1.	Напишите команду языка ассемблера процессора Intel8086 подходящую под описание: Выполнить декремент содержимого регистра CX/ECX; проанализировать регистр CX/ECX: Только если CX/ECX=0, передать управление следующей команде, если CX/ECX≠0, передать управление команде, метка которой указана в качестве операнда. Смещение метки относительно текущего значения регистра IP/EIP должно быть в диапазоне -128…+127 байт. В поле ответа вписать только команду, без операнд	**a. loop**
2.	Напишите команду языка ассемблера процессора Intel8086, единственным результатом которой является инкремент регистра eip/ip, и при этом, не имеющую операнд	**a. nop**
3.	Напишите через запятую в порядке возрастания объема одного элемента директивы объявления данных в языке ассемблера процессора Intel8086	**a. db,dw,dd,df,dq,dt** **b. db,dw,dd,dp,dq,dt** **c. db,du,dd,dp,dq,dt** **d. db,du,dd,df,dq,dt**
4.	Через запятую, без пробелов, расположите следующие регистры в порядке убывания размера: dh, spl, bl, rax, esp, ss, dil, eip, ebp, ax, rflags, sil Регистры равного размера расположите в алфавитном порядке	**a. rax,rflags,ebp,eip,esp,ax,ss,bl,dh,dil,sil,spl**
5.	Напишите команду языка ассемблера процессора Intel8086, подходящую под описание: в EIP/IP и CS загружаются значения смещения и адреса сегмента из указателя в памяти или команды. В стек заносится содержимое EIP/IP и CS.	**a. call**
6.	Напишите команды(через запятую, в алфавитном порядке, без пробелов) языка ассемблера процессора Intel8086, подходящую под описание: Реализует переход к ячейке, обозначеной операндом, при равенстве нулю флагов CF и ZF и к следующей команде в противном случае. Может использоваться как для знаковых, так и для беззнаковых чисел.	**a. JA,JNBE**
7.	Напишите команды(через запятую, в алфавитном порядке, без пробелов) языка ассемблера процессора Intel8086, подходящую под описание: Реализует переход к ячейке, обозначеной операндом, при равенстве нулю флага ZF и к следующей команде в противном случае. Может использоваться как для знаковых, так и для беззнаковых чисел.	**a. JNE,JNZ**
8.	Напишите 16битные регистры процессора Intel8086 используемые для хранения данных и выполнения различных арифметических и логических операций, разделенных на 2 части по 8-бит, с которыми можно работать как с 8-битными регистрами. Ответ напишите без пробелов, расположив регистры в алфавитном порядке.	**a. axbxcxdx**

9.	Напишите команду языка ассемблера процессора Intel8086, подходящую под описание: Над операндами приёмника и источника производится действие методом вычитания, при этом сами операнды не изменяются. По результатам данного действия устанавливаются флаги.	**a. cmp**
10.	Напишите команду языка ассемблера процессора Intel8086, подходящую под описание: Команда выполняет целочисленное деление со знаком. Делимое задается неявно, и его размер зависит от размера делителя, который явно указывается в команде. Местоположения делимого, делителя, частного и остатка — в зависимости от их размерности.	**a. idiv**
11.	Напишите команду языка ассемблера процессора Intel8086, подходящую под описание: Команда уменьшает значение регистра-указателя sp/esp, после этого записывает значение источника по адресу регистра-указателя.	**a. push**
12.	Напишите команду языка ассемблера процессора Intel8086, подходящую под описание: Передача управления по адресу, расположенному на вершине стека. Необязательный операнд число определяет количество байтов стека, которые будут вытолкнуты после выталкивания адреса возврата.	**a. ret**
13.	Напишите код создающий идентификатор с именем "Answer"(без ковычек). При ассемблированнии данный идентификатор должен замениться на вычисляемые ассемблером или компоновщиком абсолютный или относительный адрес.Данный идентификатор должен быть объявлен самым коротким способом.	**a. Answer:**
14.	Напишите через запятую, без пробелов, в алфавитном порядке специальные имена, с помощью которых возможен переход на анонимную метку.	**a. @b,@f**
15.	Объявите метку, которых в программе можно объявлять неограниченное количество, но обратиться получится только к ближайшей.	**a. @@:**
16.	В каких случаях работник предприятия может отозвать свое согласие на обработку персональных данных кадровым отделом?	a. Во всех кроме случаев, когда оформлен допуск к государственной тайне 1 формы b. Во всех кроме случаев, когда оформлен допуск к государственной тайне 2 формы c. Во всех кроме случаев, когда оформлен допуск к государственной тайне 3 формы d. Если это предусмотрено трудовым договором e. Если ранее давал письменное согласие **f. Ничего из представленного**
17.	Какие из задач информационного безопасности решает электронно-цифровая подпись?	a. конфиденциальность b. доступность **c. целостность** d. все перечисленные e. Ничего из представленного
18.	Вы сотрудник службы ИБ. Какие ситуации могут	a. выход из строя канала связи между

	восприниматься как инцидент безопасности?	офисом и провайдером b. увольнение системного администратора **c. утеря сотрудником кадрового отдела рабочего ноутбука** d. переполнение диска на файловом сервере e. сканирование портов защищаемой сети снаружи f. Ничего из представленного
19.	Кто должен знать о порядке регистрации и расследовании инцидентов безопасности?	**a. Руководящий персонал** **b. Производственный персонал** c. Только сотрудники службы ИБ d. Только руководители высшего звена e. Только сотрудники работающие сохраняемой информацией f. Только сотрудники службы охраны g. Ничего из представленного
20.	При расследовании инцидента безопасности следует ли скрывать его ход и результаты?	**a. да** b. нет, желающие должны иметь возможность ознакомится с данной информацией c. нет, все должны быть в обязательном порядке ознакомлены с данной информацией d. Ничего из представленного
21.	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 d. Ничего из представленного
22.	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 d. Ничего из представленного
23.	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 e. Ничего из представленного
24.	Какие выделяют разновидности предпосылок появления угроз?	a. случайные b. преднамеренные **c. субъективные** **d. объективные** e. Ничего из представленного
25.	Какие принципы информационной гарантированности рекомендует стратегия	**a. применение защиты во множественных местах. Поскольку**

	многоуровневой защиты:	**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.** e. Ничего из представленного
26.	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 g. Ничего из представленного
27.	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** d. Ничего из представленного
28.	На каких уровнях должны применяться меры обеспечения безопасности?	**a. законодательный** **b. административный** **c. процедурный** **d. программно-технический** e. бытовой f. Ничего из представленного
29.	Назовите основные свойства безопасности?	**a. конфиденциальность** **b. целостность** **c. доступность** d. постоянность e. равномерность f. непрерывность g. Ничего из представленного

30.	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** j. Ничего из представленного
31.	На какие виды можно подразделить аудит безопасности информационных систем?	**a. внешний аудит** **b. внутренний аудит** c. квартальный аудит d. сезонный аудит e. Ничего из представленного
32.	На каком уровне утверждается политика информационной безопасности предприятия?	a. на уровне руководителя функционального подразделения b. на уровне начальника службы ИБ c. на уровне технического директора **d. на уровне высшего руководства предприятия** e. на уровне вышестоящего или надзирающего органа f. Ничего из представленного
33.	На кого возлагается ответственность за определение подлежащих защите ресурсов на предприятии?	a. на высшее руководство **b. на руководителей среднего звена** c. на рядовых работников d. на службу ИБ e. на вышестоящие или надзирающие органы f. Ничего из представленного
34.	Может ли администратор информационной системы предприятия передавать ответственность и полномочия по обеспечению ИБ поставщику услуг?	a. нет b. полномочия - нет, ответственность - да **c. полномочия - да, ответственность - нет** d. да e. Ничего из представленного
35.	Законодательство какой страны применяется к действиям пользователей сети Интернет?	a. США b. Великобритания c. Россия d. Китай e. страны, на территории которой находится пользователь f. страны, на территории которой находится сервер

		g. страны, на территории которой зарегистрирован провайдер пользователя h. страны, на территории которой находится потерпевший (истец) i. любой страны по выбору истца j. любой страны по выбору ответчика k. страны, обозначенной в договоре между пользователем и провайдером **l. в зависимости от того, чьи интересы затронуты** m. никакое законодательство не применяется n. применяется только международное законодательство o. применяется интернет-законодательство (сетевые нормы) p. Ничего из представленного
36.	Что из перечисленного не должно отражаться в политике информационной безопасности предприятия?	a. цели защиты информации b. какие ресурсы подлежат защите c. от каких угроз защищаются ресурсы d. кто несёт ответственность за защищённость ресурсов **e. стоимость защищаемых ресурсов** f. сфера действия политики g. порядок информирования об инцидентах h. какие документы дополняют политику безопасности **i. организация взаимодействия защищаемых ресурсов** j. Ничего из представленного
37.	Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами, это?	**a. межсетевой экран** b. система обнаружения атак c. антивирусное средство d. средства контроля доступа и аутентификации
38.	Какие межсетевые экраны проверяют факт, что пакет является либо запросом на TCP-соединение, либо представляет данные, относящиеся к уже установленному соединению, либо относится к виртуальному соединению между двумя транспортными уровнями?	**a. межсетевые экраны уровня соединения** b. межсетевые экраны прикладного уровня c. межсетевые экраны с динамической фильтрацией пакетов d. межсетевые экраны инспекции состояний e. межсетевые экраны уровня ядра
39.	В случае использования межсетевого экрана уровня соединения, какая информация обычно хранится в таблице состояний после установления соединения?	**a. идентификатор сеанса** **b. состояние соединения** **c. последовательная информация** **d. IP-адрес источника и IP-адрес назначения** **e. номера портов, участвующих в сеансе** **f. физический интерфейс, куда прибыл**

		пакет **g. физический интерфейс, куда передается пакет** **h. временные метки начала открытия сеанса** i. контрольную сумму
40.	Перечислите достоинства межсетевого экрана уровня соединения.	**a. Возможность запрещения соединений с определенными хостами** **b. При использовании NAT — скрытие внутренних IP-адресов** c. Работа с протоколами высшего уровня (HTTP, FTP) d. Возможность хранения частичной информации о состоянии, полной информации состояния приложения и частичной информации о сеансе e. Возможность ограничения доступа к определенным сетевым службам f. Возможность оперирования с информацией данных пакета
41.	недостатки межсетевого экрана уровня соединения	**a. Не могут ограничить доступ протоколов, отличных от TCP** **b. Не осуществляют проверки для протоколов высших уровней** **c. Ограниченный аудит (слабая связь с высшими уровнями протоколов)** **d. Не позволяют дополнения функций — HTTP-кэширования ответов, фильтрации URL, аутентификацию** **e. Трудность тестирования правил** f. Не поддерживает NAT g. Не может запрещать соединение с определенными хостами
42.	Какие межсетевые экраны оценивают сетевые пакеты на соответствие определенному прикладному уровню перед установкой соединения? Они же исследуют данные всех сетевых пакетов на прикладном уровне и устанавливают состояние полного (завершенного) соединения и последовательной информации.	**a. межсетевые экраны прикладного уровня** b. межсетевые экраны уровня соединения c. межсетевые экраны с динамической фильтрацией пакетов d. межсетевые экраны инспекции состояний e. межсетевые экраны уровня ядра
43.	Перечислите достоинства межсетевых экранов прикладного уровня.	**a. Работа с протоколами высшего уровня (HTTP, FTP)** **b. Возможность хранения частичной информации о состоянии, полной информации состояния приложения и частичной информации о сеансе** **c. Возможность ограничения доступа к определенным сетевым службам** **d. Возможность оперирования с информацией данных пакета** **e. Запрещение прямого соединения с внешними серверами**

		f. Прозрачность proxy **g. Возможность реализации дополнительных свойств (фильтрации URL, аутентификации, кэширования HTTP)** **h. Хороший аудит**
44.	Перечислите недостатки межсетевых экранов прикладного уровня.	**a. Служба proxy требует замены сетевого стека на сервере МЭ** **b. Служба proxy слушает порт (как сетевой сервер, т.е. МЭ не может его использовать)** **c. Временная задержка (входной пакет обрабатывается дважды — приложением и proxy)** **d. Новый proxy должен быть добавлен для каждого контролируемого протокола** **e. Службы proxy обычно требуют модификации процедур клиентов** **f. Службы proxy уязвимы к ошибкам ОС и ПО прикладного уровня** **g. Не осуществляется проверка информации пакета, содержащейся в низших уровнях** **h. Служба proxy может требовать дополнительных паролей или процедур аутентификации** i. Не обеспечивает хорошего аудита j. Не поддерживает возможности оперирования с информацией данных пакета
45.	Какие межсетевые экраны позволяют осуществлять модификацию базы правил «на лету» (on fly)?	**a. межсетевые экраны с динамической фильтрацией пакетов** b. межсетевые экраны уровня соединения c. межсетевые экраны прикладного уровня d. межсетевые экраны инспекции состояний e. межсетевые экраны уровня ядра
46.	Какие межсетевые экраны имеют возможность отслеживать текущие соединения и пропускать только такие пакеты, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений?	**a. межсетевые экраны инспекции состояний** b. межсетевые экраны уровня соединения c. межсетевые экраны прикладного уровня d. межсетевые экраны с динамической фильтрацией пакетов e. межсетевые экраны уровня ядра
47.	Устройство инспекции состояний осуществляет анализ пакетов и формирование данных о «состоянии виртуального соединения». Вся информация, связанная с состоянием данного виртуального соединения, хранится в таблице динамических состояний, с помощью которой оценивается	**a. протокол, используемый для соединения** **b. IP-адреса источника и назначения** **c. номера портов источника и назначения** **d. листинг с обращенными адресами и**

	дальнейший обмен в рамках этого виртуального соединения. Когда соединение начинается с использованием отслеживаемого протокола, IP-tables добавляет записи в таблицу состояний всего соединения. Какую информацию включает в себя записи в таблице состояний?	**номерами портов** **e. время, по истечению которого соединение будет удалено** **f. состояние TCP-соединения (только для TCP)** **g. состояние отслеживаемого соединения** h. контрольную сумму
48.	Для выполнения каких задач могут быть использованы межсетевые экраны?	**a. Для защиты и изоляции приложений, сервисов и машин во внутренней сети от нежелательного трафика, приходящего из внешней сети интернет.** **b. Для ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети интернет.** **c. Для поддержки преобразования сетевых адресов.** d. Для обнаружения в реальном масштабе времени сетевых атак на сетевом уровне. e. Для обнаружения уязвимостей, позволяющих реализовать атаку.
49.	При оценке практических реализаций межсетевых экранов в качестве одного из главных параметров выступает быстродействие. Сложность проверок, осуществляемых межсетевыми экранами, обычно приводит к снижению его производительности. Какие межсетевые экраны стали разрабатываться для устранения этого существенного недостатка?	**a. межсетевые экраны уровня ядра** b. межсетевые экраны уровня соединения c. межсетевые экраны прикладного уровня d. межсетевые экраны с динамической фильтрацией пакетов e. межсетевые экраны инспекции состояний
50.	Один из основных модулей межсетевых экранов уровня ядра является ядро безопасности. Какие компоненты, составляющие суть технологии функционирования на уровне ядра, содержит ядро безопасности?	**a. перехватчик пакетов** **b. анализатор пакетов** **c. модуль верификации** **d. динамические стеки** e. модуль управления хостов f. агент регистрации входов
51.	Ядро безопасности, являющееся одним из основных модулей межсетевых экранов уровня ядра, содержит четыре компонента, составляющих суть технологии функционирования межсетевых экранов на уровне ядра. Какая из этих компонент перехватывает пакеты, поступающие на межсетевой экран, и передает их на обработку?	**a. перехватчик пакетов** b. анализатор пакетов c. модуль верификации d. динамические стеки
52.	Ядро безопасности, являющееся одним из основных модулей межсетевых экранов уровня ядра, содержит четыре компонента, составляющих суть технологии функционирования межсетевых экранов на уровне ядра. Какая из этих компонент по информации заголовка пакета подготавливает пакет и соответствующие данные для дальнейшей обработки?	a. перехватчик пакетов **b. анализатор пакетов** c. модуль верификации d. динамические стеки
53.	Ядро безопасности, являющееся одним из основных	a. перехватчик пакетов

	модулей межсетевых экранов уровня ядра, содержит четыре компонента, составляющих суть технологии функционирования межсетевых экранов на уровне ядра. Какая из этих компонент применяет заданную политику безопасности (загружаемую в ядро административным агентом), инициализирует и отслеживает сеансы всех разрешенных соединений?	b. анализатор пакетов **c. модуль верификации** d. динамические стеки
54.	Ядро безопасности, являющееся одним из основных модулей межсетевых экранов уровня ядра, содержит четыре компонента, составляющих суть технологии функционирования межсетевых экранов на уровне ядра. Какая из этих компонент зависит от конкретного протокола соединения?	a. перехватчик пакетов b. анализатор пакетов c. модуль верификации **d. динамические стеки**
55.	Выделяют несколько основных подходов к обходу межсетевых экранов. Какие?	**a. постепенный подход** **b. туннелирование** c. системный подход d. инженерный подход
56.	Под каким подходом к обходу межсетевых экранов понимается методика сбора информации об удаленной сети, защищенной межсетевым экраном? Этот метод использует посылку и анализ IP-пакетов для определения возможности определенного пакета пройти на хост назначения через устройство фильтрации пакетов. Метод позволяет определить открытые порты данного устройства, возможность прохождения пакетов для различных служб через данный порт и т.д.	**a. постепенный подход** b. туннелирование c. системный подход d. инженерный подход
57.	Под каким подходом к обходу межсетевых экранов понимается общая технология передачи протокола через общую сеть с использованием другого протокола?	a. постепенный подход **b. туннелирование** c. системный подход d. инженерный подход
58.	Применение таково подхода к обходу межсетевых экранов как туннелирование, означает использование инкапсуляции протоколов при межсетевом взаимодействии. В процессе инкапсуляции применяются три типа протоколов. Какие это типы?	**a. несущий протокол** **b. протокол-пассажир** **c. протокол инкапсуляции** d. протокол-кондуктор e. протоколы маршрутизации
59.	При межсетевом экранировании каждый IP-пакет исследуется на соответствие множеству правил. Эти правила устанавливают разрешение связи по содержанию заголовков сетевого и транспортного уровней модели TCP/IP, анализируется и направление передвижения пакета. Какие поля контролируют фильтры пакетов?	**a. физический интерфейс, откуда пришел пакет** **b. IP-адрес источника** **c. IP-адрес назначения** **d. тип транспортного уровня (TCP, UDP, ICMP)** **e. транспортные порты источника и назначения** f. контрольную сумму
60.	Отметьте правило общей схемы исследования пакетов при фильтрации:	**a. если правило разрешает, то пакет допускается** **b. если правило запрещает, то пакет удаляется** **c. если ни одно правило не применено, то пакет удаляется** d. если правило разрешает, то пакет

		удаляется e. если правило запрещает, то пакет допускается f. если ни одно правило не применено, то пакет отправляется в очередь для отложенной обработки
61.	Межсетевой экран, фильтрующий пакеты, часто переадресует сетевые пакеты так, что выходной трафик осуществляется с другими адресами. Как называется такая схема?	**a. схема трансляции адресов** b. маршрутизация c. коммутация d. схема трансформации адресов
62.	Что позволяет применение схемы NAT?	**a. спрятать топологию и схему адресации доверенной сети** **b. использовать внутри организации пул IP-адресов меньшего размера** c. обеспечивать работу протоколов маршрутизации d. обнаруживать попытки вторжения в систему
63.	Какие различают виды трансляции адресов?	**a. статическая** **b. динамическая** c. дискретная d. концентрическая
64.	Перечислите преимущества фильтрации.	**a. Быстрота работы (по сравнению с другими технологиями МЭ)** **b. МЭ может быть реализован аппаратно** **c. Не требуется конфигурирование хостов пользователя** **d. Схема NAT «прячет» внутренние IP-адреса** e. Работа с протоколами высшего уровня (HTTP, FTP) f. Хороший аудит
65.	Перечислите недостатки фильтрации.	**a. Не «понимает» прикладные протоколы** **b. Не может ограничить доступ подмножеству протоколов даже для основных служб** **c. Не отслеживает соединения (не содержит информацию о сеансе)** **d. Слабые возможности обработки информации внутри пакета** **e. Не может ограничить информацию с внутренних компьютеров к службам МЭ сервера** **f. Практически не имеет аудита** **g. Трудно тестировать правила (из-за сложности внутренних сетей, наличия различных служб)** h. Не может быть реализован аппаратно i. Не поддерживает NAT

66.	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
67.	Какие системы обнаружения вторжений осуществляют анализ активности отдельного компьютера?	a. сетевые **b. хостовые** c. гибридные d. мобильные
68.	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
69.	На какие системы обнаружения атак подразделяются по структуре?	**a. централизованные** **b. децентрализованные** c. демилитаризованные d. иерархические
70.	Какие различают системы обнаружения вторжений по характеру реакции?	**a. активные** **b. пассивные** c. перманентные d. незамедлительные
71.	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**
72.	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
73.	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
74.	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
75.	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
76.	Какие различают виды сигнатур?	**a. Сигнатуры эксплойта** **b. Сигнатуры уязвимости** **c. Сигнатуры аномалий протоколов** d. Сигнатуры анамалий
77.	действия, предпринимаемые злоумышленником, против компьютера (или сети) потенциальной жертвы, это?	**a. атака** b. вторжение c. угроза d. уязвимость
78.	Какие сигнатуры опираются на характеристики атаки, которые позволяют однозначно идентифицировать атаку?	**a. Сигнатуры эксплойта** b. Сигнатуры уязвимости c. Сигнатуры аномалий протоколов
79.	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
80.	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**
81.	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
82.	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
83.	Каковы основные методы обхода сетевых систем обнаружения вторжений?	**a. сбивание с толку** **b. фрагментация** **c. шифрование** **d. перегрузка** e. социальная инженерия
84.	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
85.	Какой метод обхода сетевых систем обнаружения	a. сбивание с толку

	вторжений заключается в разбивке пакета данных на фрагменты, которые можно послать в различном порядке (и с различными временными интервалами между ними)?	**b. фрагментация** c. шифрование d. перегрузка
86.	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
87.	Какой метод обхода сетевых систем обнаружения вторжений заключается в переполнении сетевой системы обнаружения вторжений?	a. сбивание с толку b. фрагментация c. шифрование **d. перегрузка**
88.	Несанкционированный вход в информационную систему (в результате действий, нарушающих политику безопасности или обходящих систему защиты), это?	**a. вторжение** b. атака c. угроза d. уязвимость
89.	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
90.	Как называют генерацию сигнала об обнаружении атаки (вторжения), которой не было?	**a. ложная тревога** b. пропуск c. атака d. вторжение
91.	Как называют пропуск атаки или вторжения (отсутствие сигнала тревоги при наличии вторжения)?	**a. пропуск** b. ложная тревога c. уязвимость d. вторжение
92.	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
93.	Какие выделяют подходы к обнаружению атак?	**a. обнаружение сигнатур** **b. обнаружение аномалий** **c. гибридный подход** d. обнаружение вторжений
94.	Какие выделяют виды систем обнаружения атак?	**a. хостовые** **b. сетевые** **c. гибридные** d. мобильные

95.	Какие системы обнаружения вторжений осуществляют сбор и анализ сетевых пакетов, на основании которых проводится обнаружение?	**a. сетевые** b. хостовые c. гибридные d. мобильные
96.	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
97.	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**
98.	Какое происхождение угрозы обусловливается злоумышленными действиями людей, осуществляемыми в целях реализации одного или нескольких видов угроз?	a. случайное **b. преднамеренное** c. субъективное d. объективное
99.	Какие выделяют разновидности предпосылок появления угроз?	a. случайные b. преднамеренные **c. субъективные** **d. объективные**
100.	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
101.	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

102.	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
103.	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: 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.	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
104.	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
105.	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	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**

	мотивам.	
106.	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.**
107.	Как называют интранет-сеть, подключенную к Интернету, т.е. сеть типа интранет, но санкционирующая доступ к ее ресурсам определенной категории пользователей, наделенной соответствующими полномочиями?	**a. Экстранет-сеть** b. Глобальная сеть c. Индивидуальная сеть d. Корпоративная сеть
108.	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
109.	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
110.	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
111.	Рассматривая источники угроз, как определяют	a. люди

	группу источников попадающих под следующее описание: эту группу источников рассматривают как недостатки проектирования, реализации и конфигурации (эксплуатации).	b. технические средства **c. модели, алгоритмы и программы** d. технологические схемы обработки данных e. внешняя среда
112.	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
113.	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**
114.	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**
115.	Какие виды утечки выделяют в соответствии с ГОСТ 50922-96?	**a. разглашение** **b. несанкционированный доступ к информации** **c. получение защищаемой информации разведками**
116.	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
117.	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
118.	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
119.	С помощью чего может осуществляться получение защищаемой информации разведками?	**a. технические средства** **b. агентурные методы** c. воздушные средства d. методы глубокого анализа
120.	Что называют совокупностью источника информации, материального носителя или среды	**a. канал утечки информации** b. информационный канал

	распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя?	c. уязвимый канал
121.	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.
122.	На каких уровнях должны применяться меры обеспечения безопасности?	**a. законодательный** **b. административный** **c. процедурный** **d. программно-технический** e. бытовой
123.	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**
124.	Назовите основные свойства безопасности?	**a. конфиденциальность** **b. целостность** **c. доступность** d. постоянность e. равномерность f. непрерывность
125.	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
126.	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
127.	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
128.	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
129.	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
130.	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**
131.	Какие типы сетевых периметров можно выделить?	**a. внешний** **b. внутренний** c. кольцевой d. федеральный

132.	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
133.	Какой тип сетевого периметра представляет собой дополнительные границы, в которых размещаются другие механизмы безопасности, такие как МЭ и фильтрующие маршрутизаторы?	**a. Внутренний сетевой периметр** b. Внешний сетевой периметр c. Территориальный сетевой периметр d. Иерархический сетевой периметр
134.	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
135.	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
136.	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
137.	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
138.	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
139.	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
140.	Нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им основных своих функций, это?	**a. Отказ** b. Сбой c. Ошибка d. Побочное влияние
141.	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
142.	Неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций, происходящее вследствие специфического	a. Отказ b. Сбой **c. Ошибка**

	(постоянного или временного) его состояния, это?	d. Побочное влияние
143.	Как называется подключение, установленное по существующей общедоступной инфраструктуре и использующее шифрование и аутентификацию для обеспечения безопасности содержания передаваемых пакетов?	**a. Виртуальные частные сети** b. Удаленное подключение c. Пиринговые сети d. Файлообменная сеть
144.	Как называется режим подключения по протоколу IPSec, при котором используется форма связи типа узел-узел, где применяется шифрование только содержательной части пакета? Этот режим VPN удобно использовать для зашифрованной связи между узлами одной сети.	**a. транспортный режим** b. туннельный c. статичный d. динамичный e. монолитный
145.	Как называется режим подключения по протоколу IPSec, который применяется при создании большинства VPN, потому что он шифрует весь оригинальный пакет? Данный режим может применяться для организации связи типа узел-узел, узел-шлюз или шлюз-шлюз.	**a. режим туннелирования** b. транспортный режим c. статичный d. динамичный e. монолитный
146.	Как называется стандартный протокол IPsec, используемый для обеспечения безопасности взаимодействия в виртуальных частных сетях? Его предназначение — защищенное согласование и доставка идентифицированного материала для ассоциации безопасности (SA).	**a. IKE (Internet Key Exchange)** b. SPD (Security Policy Database) c. SAD (Security Association Database) d. SPI (Security Parameter Index)
147.	Установление безопасного соединения начинается с формирования ассоциации обеспечения безопасности (Security Association, SA) между двумя сообщающимися сторонами. Прежде чем договариваться об ассоциации обеспечения безопасности, необходимо локальное конфигурирование элементов протокола IPSec, которые данный партнер собирается поддерживать. Где хранятся эти параметры настройки?	**a. в базе данных политики безопасности (Security Policy Database, SPD)** b. в базе данных ассоциации обеспечения безопасности (Security Association Database, SAD) c. в виде уникального индекса параметра обеспечения безопасности (Security Parameter Index, SPI)
148.	На какой фазе протокола IKE удаленный пользователь начинает сеанс со шлюзовым устройством VPN? Эта фаза выполняет две функции: аутентификацию удаленного пользователя и обмен информацией об открытых ключах.	**a. на первой фазе** b. на второй фазе c. на третьей фазе d. на четвертой фазе
149.	В первой фазе при обмене аутентификационной информацией и параметрами безопасности могут использоваться несколько режимов. Различия между ними заключаются в количестве сетевых пакетов, которыми обмениваются стороны, и во времени, за которое генерируется открытый ключ. Назовите эти режимы.	**a. основной** **b. агрессивный** c. транспортный d. туннельный
150.	На какой фазе протокола IKE согласовываются конкретные параметры ассоциации обеспечения безопасности IPSec? После завершения этой фазы формируется ассоциация обеспечения безопасности (SA) и пользователь получает подключение к VPN.	a. на первой фазе **b. на второй фазе** c. на третьей фазе d. на четвертой фазе
151.	Какой протокол можно отнести к протоколу VPN транспортного уровня?	**a. SSL/TLS (Secure Socket Layer/Transport Layer Security)** b. IPSec (IPSec Protocol Suite) c. PPTP (Point-to-point Tunneling Protocol)

		d. L2TP (Layer Two Tunneling Protocol)
152.	Для организации защищенных связей необходимо применение шифрования, которое, в свою очередь, требует наличия у пользователя ключа шифрования. При этом возникает проблема управления ключами. Какие задачи включается в себя данная проблема?	**a. генерацию** **b. проверку** **c. распространение** **d. использование** **e. хранение** **f. резервирование** **g. обновление** **h. уничтожение ключей** **i. установление времени жизни ключа**
153.	Как называется выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов?	**a. цифровой сертификат** b. ключ шифрования c. открытый ключ d. закрытый ключ
154.	На какие основных типа можно подразделить по конфигурации VPN?	**a. узел-узел (host-to-host)** **b. узел-шлюз (host-to-gateway)** **c. шлюз-шлюз (gateway-to-gateway)**
155.	Какой тип VPN можно использовать для организации канала связи проходящего через Интернет?	**a. узел-узел (host-to-host)** **b. узел-шлюз (host-to-gateway)** **c. шлюз-шлюз (gateway-to-gateway)**
156.	Как называется процесс инкапсуляции одного типа пакетов внутри другого в целях получения некоторого преимущества при транспортировке?	**a. туннелирование** b. шифрование c. аутентификация d. процесс соединения
157.	Какие можно отметить недостатки VPN?	**a. накладные расходы обработки данных** **b. пакетные накладные расходы** **c. проблемы реализации, связанные с применением трансляции сетевых адресов для VPN, с размером максимального блока передачи данных** **d. проблемы управления и поиска конфликтов** **e. проблемы с функционированием сетевых систем обнаружения вторжений** f. нарушение конфиденциальности информации
158.	Какие протоколы реализации VPN существуют на канальном уровне?	**a. протокол туннелирования типа «точка-точка» (Point-to-point Tunneling Protocol, PPTP)** **b. протокол туннелирования второго уровня (Layer Two Tunneling Protocol, L2TP)** c. набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP (IP Security, IPSec)

		d. Криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером (Secure Sockets Layer, SSL)
159.	В какие этапы происходит формирование защищенного канала?	**a. установление соединения клиента с сервером удаленного доступа** **b. аутентификация пользователя** **c. конфигурирование защищенного туннеля** d. оценка эффективности защищенного туннеля e. анализ объектов защиты
160.	Как называется набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP? Он позволяет осуществлять подтверждение подлинности и/или шифрование IP-пакетов, а также включает в себя протоколы для защищённого обмена ключами в сети Интернет.	**a. IPSec (IPSec Protocol Suite)** b. PPTP (Point-to-point Tunneling Protocol) c. L2TP (Layer Two Tunneling Protocol) d. SSL (Secure Sockets Layer)
161.	Какие основные режимы имеет подключение по протоколу IPSec?	**a. транспортный** **b. туннельный** c. статичный d. динамичный e. монолитный
162.	Что организация ценит и хочет защитить?	**a. Ресурсы** b. Честь c. Уязвимости d. Контроль безопасности
163.	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
164.	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	**a. средства автоматического сканирования уязвимостей** **b. тесты и оценка безопасности** **c. тесты на проникновение** d. средства удаленного

	включают в себя методы тестирования?	администрирования
165.	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
166.	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
167.	Что может использоваться для оценки контроля безопасности и уверенности в том, что различные аспекты ИТ системы защищены?	a. средства автоматического сканирования уязвимостей b. тесты и оценка безопасности **c. тесты на проникновение**
168.	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
169.	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
170.	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
171.	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
172.	На основе чего выбираются средства защиты (контроля), которые могут уменьшить или устранить идентифицированный риск?	**a. матрицы уровней риска** b. результатов идентификации угроз c. результатов идентификации уязвимостей d. анализа влияния
173.	Как называют потенциальную причину нежелательного события, которое может нанести ущерб организации и ее объектам?	**a. Угроза** b. Уязвимость c. Риск безопасности d. Ресурс
174.	Посредством применения каких операций можно достигнуть уменьшения риска?	**a. принятие риска** **b. уклонение от риска** **c. ограничение риска** **d. планирование риска** **e. исследования и подтверждения** **f. передача риска**
175.	Посредством чего организация может получить допустимый остаточный риск?	**a. удаления некоторых системных уязвимостей (дефектов и слабостей) путем уменьшения числа возможных пар источник угрозы—уязвимость** **b. добавления специальных нацеленных средств для уменьшения способности и мотивации источника угроз** **c. уменьшения величины нежелательного влияния**
176.	Как называют системный процесс получения и оценки объективных данных о текущем состоянии системы (технологий), действиях и событиях, происходящих в ней, который устанавливает уровень их соответствия определенному критерию и предоставляет результаты заказчику?	**a. Аудит информационной системы** b. Тест на проникновение c. Внутренний аудит d. Внешний аудит
177.	Перечислите основные информационные активы организации?	**a. идеи** **b. знания** **c. проекты** **d. результаты внутренних обследований**
178.	На какие виды можно подразделить аудит безопасности информационных систем?	**a. внешний аудит** **b. внутренний аудит** c. квартальный аудит d. сезонный аудит
179.	Какой вид аудита используется для проведения вне организации и, как правило, специализированными организациями, занимающимися аудитом	**a. внешний аудит** b. внутренний аудит c. квартальный аудит

	информационной безопасности?	d. сезонный аудит
180.	Что относится к основным компонентам безопасности, комбинация которых обеспечивает защиту от атак на целостность, конфиденциальность и доступность?	**a. межсетевые экраны** **b. системы обнаружения вторжений** **c. средства контроля целостности** **d. средства проверки содержимого** **e. сканеры** **f. средства контроля конфигураций** **g. средства контроля доступа и аутентификации** **h. виртуальные частные сети**
181.	Какие виды угроз можно выделить?	**a. естественные** **b. преднамеренные** **c. случайные** d. паранормальные
182.	Слабости, ассоциированные с ресурсами организации, это?	**a. Уязвимости** b. Угроза c. Риск безопасности d. Ущерб
183.	Как называется возможность данной угрозы реализовать уязвимости для того, чтобы вызвать ущерб или разрушение ресурса или группы ресурсов, что прямо или косвенно воздействует на организацию?	**a. Риск безопасности** b. Контроль безопасности c. Ресурс d. Уязвимость
184.	Какие шаги включает в себя общая оценка риска?	**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** j. выявление ресурсного фонда
185.	Типы уязвимостей и методологии их определения обычно зависят от природы информационных технологий системы и фазы ее жизненного цикла. Какая методология используется, если ИТ система еще не спроектирована?	**a. Поиск уязвимостей концентрируется на организационной политике безопасности, планируемых процедурах безопасности, определении системных требований и анализе документов поставщиков продуктов безопасности.** b. Идентификация уязвимостей должна быть расширена для включения дополнительной информации, такой, например, как соответствие свойств безопасности, описанных в документации по безопасности, результатам сертификационных тестов и испытаний. c. Процесс идентификации уязвимостей

		должен включать в себя анализ свойств безопасности ИТ системы и контроля безопасности (технического и процедурного), используемого для защиты системы.
186.	Типы уязвимостей и методологии их определения обычно зависят от природы информационных технологий системы и фазы ее жизненного цикла. Какая методология используется, если ИТ система уже применяется?	**a. Идентификация уязвимостей должна быть расширена для включения дополнительной информации, такой, например, как соответствие свойств безопасности, описанных в документации по безопасности, результатам сертификационных тестов и испытаний.** b. Поиск уязвимостей концентрируется на организационной политике безопасности, планируемых про-цедурах безопасности, определении системных требований и анализе документов поставщиков продуктов безопасности. c. Процесс идентификации уязвимостей должен включать в себя анализ свойств безопасности ИТ системы и контроля безопасности (технического и процедурного), используемого для защиты системы.
187.	Типы уязвимостей и методологии их определения обычно зависят от природы информационных технологий системы и фазы ее жизненного цикла. Какая методология используется, если ИТ система функционирует?	**a. Процесс идентификации уязвимостей должен включать в себя анализ свойств безопасности ИТ системы и контроля безопасности (технического и процедурного), используемого для защиты системы.** b. Поиск уязвимостей концентрируется на организационной политике безопасности, планируемых про-цедурах безопасности, определении системных требований и анализе документов поставщиков продуктов безопасности. c. Идентификация уязвимостей должна быть расширена для включения дополнительной информации, такой, например, как соответствие свойств безопасности, описанных в документации по безопасности, результатам сертификационных тестов и испытаний.

4. Порядок проведения и критерии оценивания промежуточной аттестации

4.1. Порядок проведения промежуточной аттестации

Экзамен проводится в виде тестирования. Студент должен ответить на вопросы закрытого типа, которые предполагают выбор вариантов ответа, а также на вопросы открытого типа, которые не предполагают вариантов ответа, правильный ответ требуется написать самостоятельно. Всего 20 тестовых вопросов. Продолжительность теста – 35 минут.

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

4.2.1. Критерии оценивания теста

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

Оценка	Отлично/ Зачтено	Хорошо/ зачтено	Удовлетворительно/зачтено	Неудовлетворительно/ незачтено
Баллы	100-91 баллов	90-76 баллов	75-60 баллов	59-0 баллов
Уровень освоения проверяемых компетенций	высокий	средний	базовый	недостаточный

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

Итоговая оценка за семестр формируется следующим образом:
Каждая практическая работа с 1 по 6 оценивается в 8 балла итоговой оценки. Итоговый тест дает 52 балла итоговой оценки. Максимум можно набрать 100 баллов за семестр.

Итоговая оценка конвертируется в 5 бальную систему:

Набранная сумма баллов - оценка
Менее 60 – неудовлетворительно;
60-75 – удовлетворительно (зачет);
76-89 – хорошо (зачет);
90-100 – отлично (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 отлично:

- предполагает формирование компетенций на высоком уровне;

- знание теоретических разделов изучаемой дисциплины на уровне не ниже оценки отлично;
- 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. Средний уровень соответствует оценке хорошо:
- предполагает формирование компетенций на среднем уровне;
- знание теоретических разделов изучаемой дисциплины на уровне не ниже оценки хорошо;
- студент умеет применять знания, полученные в рамках изучения дисциплины, для решения задач профессиональной деятельности;

3. Базовый уровень соответствует оценке удовлетворительно:
- предполагает формирование компетенций на базовом уровне;
- знание теоретических разделов изучаемой дисциплины на уровне не ниже оценки удовлетворительно;

4. Недостаточный уровень соответствует оценке неудовлетворительно.