МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета математики
и компьютерных наук имени
профессора Н.И. Червякова
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Программно-аппаратные средства защиты информации
название дисциплины (модуля)

Направление подготовки	10.03.01 «Информационная безопасность»
Направленность (профиль)	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	5,6

Введение

1. Назначение. Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Программно-аппаратные средства защиты информации» студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

2. ФОС является приложением к программе дисциплины (модуля) «Программно-аппаратные средства защиты информации» в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

3. Разработчик (и) Орел Д.В., доцент кафедры

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены комиссии: Жук А.П., профессор кафедры
Минкина Т.В., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «Инфоком-С»

Экспертное заключение: Фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Программно-аппаратные средства защиты информации».
Место для ввода даты.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенции(й),			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
Компетенция: ОПК-9 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности				
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-3 ОПК-9 Выбирает оптимальный вариант использования навыков и методик применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности*	- не достаточно знает устройство и принципы работы криптографических средств защиты информации, применяемых в компьютерных системах и сетях; - затрудняется с установкой, настройкой и интеграцией криптографические средства защиты информации в компьютерных системах и сетях	- имеет общее представление об устройстве и принципах работы криптографических средств защиты информации, применяемых в компьютерных системах и сетях; - со значительными недочётами устанавливает, настраивает и интегрирует криптографические средства защиты информации в компьютерных системах и сетях	- в основном знает устройство и принципы работы криптографических средств защиты информации, применяемых в компьютерных системах и сетях; - с незначительными недочётами устанавливает, настраивает и интегрирует криптографические средства защиты информации в компьютерных системах и сетях	- знает устройство и принципы работы криптографических средств защиты информации, применяемых в компьютерных системах и сетях; - устанавливает, настраивает и интегрирует криптографические средства защиты информации в компьютерных системах и сетях

Результаты обучения по дисциплине (модулю): *Индикатор: ИД-1 ОПК-10 Использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности*	- затрудняется с использованием федеральных, отраслевых и ведомственных нормативных документов для формирования политики информационной безопасности; - затрудняется с использованием нормативно-правовых документов при разработке положений, приказов, инструкций и других документов, реализующих политику информационной безопасности; - не способен принимать участие в организации работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты информации	- со значительными неточностями использует федеральные, отраслевые и ведомственные нормативные документы для формирования политики информационной безопасности; - со значительными неточностями использует нормативно-правовые документы при разработке положений, приказов, инструкций и других документов, реализующих политику информационной безопасности; - в целом способен принимать участие в организации работоспособности и эффективности применяемых программных, программно-аппаратных средств защиты информации	- с незначительными неточностями использует федеральные, отраслевые и ведомственные нормативные документы для формирования политики информационной безопасности; - с незначительными неточностями использует нормативно-правовые документы при разработке положений, приказов, инструкций и других документов, реализующих политику информационной безопасности; - способен принимать участие в организации работоспос	- использует федеральные, отраслевые и ведомственные нормативные документы для формирования политики информационной безопасности; - использует нормативно-правовые документы при разработке положений, приказов, инструкций и других документов, реализующих политику информационной безопасности; - способен принимать участие в организации работоспособности и эффективности применяемых программных, программн

			обности и эффективности применяемых программных, программно-аппаратных средств защиты информации	о-аппаратных средств защиты информации

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения ОФО семестр 5, 6,	*ОПК-9*
1.		Модель контроля целостности Кларка-Вилсона.	ОПК-9
2.		Модель безопасности на основе матрицы доступов HRU.	ОПК-9
3.		Модель распространения прав доступа TAKE-GRANT.	ОПК-9
4.		Модель системы безопасности Белла-Лападула.	ОПК-9
5.		Модель безопасности информационных потоков.	ОПК-9
6.		Модели нарушителя информационных систем.	ОПК-9
7.		Модели нарушения целостности программ и данных в элек¬тронно-вычислительныхмашинах.	ОПК-9
8.		Теория безопасных систем. ТСВ.	ОПК-9
9.		Политики безопасности. Домены безопасности. Основные типы.	ОПК-9
10.		Парольная защита Требования и атаки.	ОПК-9
11.		Криптографические методы защиты. Основные требования, модели, способы иреализации.	ОПК-9
12.		Асимметричное шифрование. Модели и алгоритмы.	ОПК-9
13.		Симметричное шифрование. Модели и алгоритмы.	ОПК-9
14.		Электронно-цифровая подпись. Модели, требования, атаки, способы обмана,	ОПК-9

		реализацияЭЦП.	
15.		Криптографические атаки на схемы шифрования.	ОПК-9
16.		Критерии оценки безопасности компьютерных систем мини¬стерства обороны США(«Оранжевая книга»).	ОПК-9
17.		Европейские критерии безопасности информационных тех¬нологий.	ОПК-9
18.		Федеральные критерии безопасности информационных тех¬нологий.	ОПК-9
19.		Руководящие документы Государственной Технической Ко¬миссии при Президенте РФ.	ОПК-9
20.		Защита распределенных баз данных: транзакция, репликация, резервирование и другиеособенности по надежности.	ОПК-9
21.		Общие положения криптографии. Имитостойкость, имитозащита.	ОПК-9
22.		Криптографические алгоритмы. Перемешивания и рассеивания. Подстановки.	ОПК-9
23.		Реализация шифров. Методы получения случайных и псевдослучайных чисел.	ОПК-9
24.		Блочные и поточные шифры на основе реализации требований ГОСТ 28147-99	ОПК-9
25.		Блочные и поточные шифры на основе симметричных криптографических алгоритмов.	ОПК-9
26.		Методы анализа симметричных криптосистем.	ОПК-9
27.		Методы криптоанализа несимметричных криптосистемПротокол SSH.	ОПК-9

28.		Применение криптографических алгоритмов для обеспечения безопасности информациив информационных системах. Технология VPN.	ОПК-9
29.		Технологии WPA и WPA2.	ОПК-9
30.		Применение криптографических алгоритмов для обеспечения безопасности информациив информационных системах.	ОПК-9
31.		Основы технологии инфраструктуры открытых ключей.	ОПК-9
32.		Основные компоненты и сервисы ИОК.	ОПК-9
33.		Введение в компьютерные атаки. Модель атаки. Результат атаки.	ОПК-9
34.		Атаки с использованием промежуточных узлов и территорий.	ОПК-9
35.		Технологии обнаружения компьютерных атак и их возможности.	ОПК-9
36.		Модели нарушителей информационной безопасности	ОПК-9
37.		Модели угроз информационной безопасности	ОПК-9
38.		Программные закладки. Классификация, воздействие на компьютерную систему.	ОПК-9
39.		Методы защиты от программных закладок.	ОПК-9
40.		Методы защиты компьютерной системы от взлома.	ОПК-9
41.		Назначение межсетевых экранов.	ОПК-9
42.		Уровни сетевой модели, на которых применяется фильтрация пакетов.	ОПК-9
43.		Статическая и динамическая трансляция адресов.	ОПК-9

44.		Значение функции трансляции адресов с точки зрения обеспечения информационнойбезопасности.	ОПК-9
45.		Предотвращение взлома компьютерной системы на уровне СУБД	ОПК-9
46.		Предотвращение взлома компьютерной системы на уровне операционной системы.	ОПК-9
47.		Политика ИБ и политика СУИБ: сходства и различия.	ОПК-9
48.		Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура,дополнительные роли в рамках процессов управления ИБ.	ОПК-9
49.		Анализ рисков ИБ: основные понятия	
50.	A, b	Какие из приведенных утверждений характеризуют цифровую гигиену a) образ мышления и привычки с фокусом на безопасность b) помогает пользователям и организациям снизить количество нарушений в интернете c) регулярные меры предосторожности для обеспечения здоровья и благополучия d) все вышеперечисленное	ОПК-9
51.	A, b, c, d	Проблемы, решаемые с помощью кибергигиены a) Нарушения конфиденциальности данных b) Потеря данных c) Устаревшее программное обеспечение d) Устаревший антивирус	ОПК-9
52.	d	Какими путями можно добиться регулярности выполнения процедур кибергигиены a) выработка привычек b) автоматические напоминания	ОПК-9

		c) добавлять в календарь даты выполнения разных задач d) все перечисленное	
53.	a	Какой из перечисленных инструментов не относится к кибергигиене a) Рециркулятор b) Сетевой экран c) Менеджер паролей d) Антивирусное программное обеспечение	ОПК-9
54.	a	Какой пароль можно считать надёжным a) Длинный пароль, использующий большой алфавит символов b) Короткий пароль, использующий большой алфавит символов c) Длинный пароль, использующий малый алфавит символов d) Короткий пароль, использующий малый алфавит символов	ОПК-9
55.	a	Для чего используется программное обеспечение для удаления данных a) При утилизации компьютера удаляются данные, чтобы случайно не попали в чужие руки b) При заполнении жётского диска удаляются данные, чтобы очистить место c) При замедлении работы компьютера удаляются данные, чтобы очистить место d) При возникновении желания пользователя удаляются данные, чтобы очистить место	ОПК-9
56.	d	Чек-лист правил кибергигиены не включает следующий пункт a) Хранение паролей в безопасности b) Использование многофакторной аутентификации c) Регулярное резервное копирование данных d) Обеспечение общего доступа к файлам и каталогам	ОПК-9
57.	d	Обеспечение конфиденциальности не включает следующий пункт a) Не публиковать в социальных сетях личную информацию, такую как домашний адрес, личные фотографии, номер телефона, номера кредитных карт b) Оценить настройки конфиденциальности в социальных сетях и убедиться, что они установлены на комфортном для вас уровне	ОПК-9

		c) Избегать викторин, игр и опросов в социальных сетях, где запрашивается конфиденциальная личная информация d) Не блокировать компьютер и телефон с помощью пароля или PIN-кода	
58.	c	Защита от атак социальной инженерии не включает следующий пункт a) Не переходить по подозрительным ссылкам, в которых вы не уверены b) Не открывать письма, выглядящие подозрительно c) Не блокировать загрузку подозрительных вложений в сообщениях электронной почты и текстовых сообщениях, которых вы не ждете d) Не переходить по объявлениям, обещающим бесплатные деньги, призы и скидки	ОПК-9
59.	C, d	Установка одновременно нескольких антивирусов повышает защищённость a) Да b) Да, если антивирусы от известных производителей c) Нет + d) Антивирусы могут мешать работе друг друга	ОПК-9
60.	a	Двухфакторная аутентификация - это a) Предоставление двух независимых средств идентификации перед получением доступа b) Пароль, введённый 2 раза подряд c) Пароль, состоящий из двух слов d) Антивирус	ОПК-9
61.	a	Технология, обеспечивающая конфиденциальность данных в сети Интернет - это a) Шифрование b) Авторизация c) Аутентификация d) Идентификация	ОПК-9
62.	b	Что такое Botnet a) Вредоносная программа, которая маскирует себя среди других файлов или данных, хранящихся на компьютере b) Группа компьютеров, на которых работают вредоносные программы, удаленно управляемые киберпреступниками	ОПК-9

		c) Новый тип вируса, создающий хаос по всему миру	
63.	d	Что из перечисленного является примером фишинга a) Письмо по электронной почте от человека, с которым вы редко контактируете, содержащее только ссылку на web адрес b) Сообщение о том, что вы выиграли в конкурсе, и для получения приза нужно перейти по предложенной ссылке c) Письмо по электронной почте с просьбой ввести данные аутентификации в системе дистанционного банковского обслуживания, но адрес отправителя не похож на адрес вашего банка d) Все вышеперечисленное	ОПК-9
64.	c	Чтобы ваш смартфон и данные оставались защищёнными и безопасными, при установке новых приложений рекомендуется a) Заблокировать все загрузки приложений и использовать стандартное приложение, уже имеющееся в вашем смартфоне b) Не использовать слишком много приложений, так как станет смартфон менее безопасным c) Изучить внимательно запросы на разрешение при использовании или установке приложений для смартфона	ОПК-9
65.	c	Гарантирует ли режим «Инкогнито» конфиденциальность навигации в Интернете a) Конечно! Никто не сможет узнать, что я делал в Интернете b) Только Интернет-провайдер знает, что я делал c) Режим конфиденциального просмотра защищает только от несанкционированного физического доступа к компьютеру	ОПК-9
66.	b	Какие действия рекомендуется предпринять в случае временного оставления рабочего места для предотвращения несанкционированного доступа к компьютеру a) Получить разрешения Руководителя покинуть рабочее место b) Использовать комбинацию клавиш Ctrl-Alt-Del или режим Lock Computer c) Выключить компьютер d) Отключить монитор	ОПК-9

67.	c	Какие типы атак приводят к нарушению нормальной работы веб-сайта или другого сетевого ресурса a) Атака POS b) Фишинг c) Атака DoS d) Все перечисленные	ОПК-9
68.	c	С какими угрозами информационной безопасности может быть связано использование файлов Cookie a) Они могут собирать данные, хранящиеся на компьютере b) Они могут содержать вирусы и инфицировать компьютер c) Они могут содержать персональные данные и привести к угрозе подмены идентичности пользователя d) Все перечисленное	ОПК-9
69.	c	Обеспечение безопасности роутеров не включает следующий пункт a) Изменить имя, заданное по умолчанию для домашней сети Wi-Fi b) Изменить имя пользователя и пароль роутера c) Использовать первоначальную прошивку без обновлений d) Отключить удаленный доступ, универсальную настройку сетевых устройств (Universal Plug and Play) и настройку защищенного Wi-Fi	ОПК-9
70.	d	Для чего назначается идентификатор маршрутизатора ID a) на основе ID протокол OSPF прокладывает маршруты b) идентификатор маршрутизатора ID запускает процесс маршрутизации c) идентификатор ID служит для организации обмена Hello-пакетами d) идентификатор маршрутизатора используется при выборе DR и BDR	ОПК-9
71.	d	Что нельзя выполнить в окне Изменение параметров домашней группы a) выйти из домашней группы b) изменить пароль c) открыть общий доступ к документам d) создать домашнюю группу	ОПК-9
72.	b	Какой из протоколов задает набор правил для отправки электронной почты a) POP протокол b) SMTP протокол	ОПК-9

		c) TCP/IP d) протокол DHCP	
73.	b	При сохранении карты сети в файл, какое она получает расширение a) *.avi b) *.ndf c) *.doc d) *.png	ОПК-9
74.	c	Политика безопасности – это a) Совокупность административных мер, которые определяют порядок прохода в компьютерные классы b) Множество критериев для предоставления сервисов безопасности c) Совокупность как административных мер, так и множества критериев для предоставления сервисов безопасности d) Межсетевые экраны, используемые в организации	ОПК-9
75.	a	Межсетевые экраны прикладного уровня могут a) Выполнять аутентификацию пользователя b) Автоматически распознавать новые протоколы c) Шифровать данные пользователя d) Выполнять авторизацию пользователя	ОПК-9
76.	a	Политика межсетевого экрана определяет a) Как межсетевой экран будет обрабатывать сетевой трафик для определенных IP-адресов и диапазонов адресов, протоколов, приложений и типов содержимого b) Как межсетевой экран будет маршрутизировать пакеты c) Как межсетевой экран будет обеспечивать качество обслуживания (QoS) d) Как межсетевой экран будет обеспечивать балансировку нагрузки	ОПК-9
77.	d	Трансляция сетевых адресов (NAT) позволяет a) Скрыть логины пользователей локальной сети b) Скрыть пароли пользователей локальной сети c) Скрыть сетевой адрес самого межсетевого экрана d) Скрыть схему сетевой адресации локальной сети	ОПК-9

78.	A, d	Основные принципы, которым необходимо следовать при разработки окружения межсетевого экрана a) Необходимо сделать окружение межсетевого экрана максимально простым b) Необходимо сделать окружение межсетевого экрана максимально сложным c) Не следует использовать системы обнаружения проникновения d) Необходимо предусмотреть дополнительные инструментальные средства обеспечения безопасности	ОПК-9
79.	A, d	При использовании IDS a) Возрастает возможность определения преамбулы атаки b) Возрастает возможность фильтрования трафика c) Возрастает возможность определения оптимального маршрута для каждого кадра d) Возрастает возможность раскрытия осуществленной атаки	ОПК-9
80.	a	Системы анализа уязвимостей используются a) Для создания «моментального снимка» состояния безопасности системы b) Как альтернатива IDS, полностью заменяя ее c) Как альтернатива политики безопасности предприятия, являясь полным ее аналогом d) Как альтернатива межсетевым экранам, полностью заменяя их	ОПК-9
81.	b	Создание альтернативных маршрутов основано на следующих принципах a) В дополнение к основной таблице маршрутизации main, созданной по умолчанию, можно определить несколько альтернативных таблиц маршрутизации b) Для выбора конкретной таблицы маршрутизации используются Routing Rules, в которых указывается соответствие между типом трафика и используемой для его маршрутизации таблицей c) Альтернативные таблицы маршрутизации создаются вместо основной таблицы main d) Альтернативные таблицы маршрутизации предназначены для замены правил фильтрования	ОПК-9
82.	b	Конфиденциальность – это	ОПК-9

		a) Невозможность несанкционированного изменения данных b) Невозможность несанкционированного просмотра данных c) Невозможность несанкционированного выполнения программ d) Невозможность несанкционированного доступа к данным	
83.	b	Широковещательными пакетами называются пакеты, у которых a) В части IP-адреса получателя, относящейся к номеру сети, стоят все единицы b) В части IP-адреса получателя, относящейся к номеру хоста, стоят все единицы c) В части IP-адреса получателя, относящейся к номеру хоста, стоят все нули d) В части IP-адреса получателя, относящейся к номеру сети, стоят все нули	ОПК-9
84.	b	Основное назначение межсетевого экрана состоит в том, чтобы a) Обеспечить полную безопасность локальной сети b) Защитить хосты и сети от использования существующих уязвимостей в стеке протоколов TCP/IP c) Обнаружить проникновение в локальную сеть d) Выполнить аутентификацию пользователей	ОПК-9
85.	a	Что из перечисленного всегда является уязвимостью a) Слабое место в системе, с использованием которого может быть осуществлена атака b) Ошибка в программном обеспечении c) Отсутствие политики безопасности d) Ошибка в настройках межсетевого экрана	ОПК-9
86.	C, d	Межсетевые экраны прикладного уровня a) Должны иметь агента для каждого уровня модели OSI b) Могут быть реализованы исключительно программно c) Анализируют содержимое прикладного уровня d) Должны иметь агента для каждого прикладного протокола	ОПК-9
87.	a	Политика по умолчанию для всего трафика должна быть a) Deny (Drop) b) Allow c) Accept	ОПК-9

		d) Forward	
88.	a	Если на хосте ESXI включен режим строгой блокировки, какое действие должен выполнить администратор, чтобы пользователям с правами администратора разрешить доступ к оболочке ESXI или SSH a) добавить пользователей в список исключений b) включить службу, чтобы разрешить доступ к оболочке ESXi или SSH + c) очистить список исключений d) создать пользователей с соответствующими правами	ОПК-9
89.	a	ИТ-администратор настроил два сервера vCenter в пределах PSC и должен предоставить пользователю право доступа ко всем средам. Какой уровень доступа нужно выдать для этого a) требуется глобальное разрешение на доступ ко всем средам b) требуется локальное разрешение на доступ к PSC серверу c) требуется очистить список исключений d) нет правильного варианта	ОПК-9
90.	a	Маршрутизатор NAT a) Расположен на границе между двумя областями адресов и преобразует адреса в IP-заголовках таким образом, что пакет корректно маршрутизируется при переходе из одной области в другую b) Расположен на границе между двумя областями адресов, в одной из которых адреса принадлежат частной сети, а в другой – внешней c) Расположен на границе между локальной сетью и интернетом d) Расположен на границе между двумя локальными сетями с разными требованиями к безопасности	ОПК-9
91.	b	Типичная ситуация, когда требуется несколько уровней межсетевых экранов a) Наличие нескольких помещений, в которых расположены рабочие станции пользователей b) Наличие внутренних пользователей с различными уровнями доверия + c) Наличие как входящего, так и исходящего трафика d) Наличие внутренних пользователей, аутентификация которых выполняется различными способами	ОПК-9
92.	A, b	Преимущества использования IDS	ОПК-9

		a) Возможность иметь реакцию на атаку b) Возможность блокирования атаки c) Выполнение документирования существующих угроз для сети и систем + d) Нет необходимости в межсетевых экранах	
93.	a	Общие свойства системам анализа уязвимостей и системам обнаружения проникновения a) И те, и другие следят за конкретными симптомами проникновения и другими нарушениями политики безопасности b) И те, и другие могут фильтровать трафик c) И те, и другие могут шифровать трафик d) И те, и другие могут аутентифицировать пользователей	ОПК-9
94.	A, b	Альтернативные таблицы маршрутизации содержат a) Информацию, аналогичную информации в таблице main b) Дополнительный параметр Ordering, который определяет порядок просмотра данной таблицы маршрутизации и таблицы main c) Дополнительный параметр Accounting, который определяет список пользователей, трафик которых маршрутизируется с использованием альтернативной таблицы d) Дополнительный параметр Filtering, который определяет правила фильтрования для пакетов, маршрутизируемых в соответствии с данным правилом	ОПК-9
95.	b	Уменьшение количества хостов в широковещательном домене необходимо a) Для обеспечения конфиденциальности трафика b) Для предотвращения «широковещательных штормов» c) Для предотвращения несанкционированного доступа d) Для обеспечения более строгой аутентификации	ОПК-9
96.	d	Межсетевые экраны являются a) Специализированными программами, невозможна аппаратная реализация b) Специализированными аппаратными устройствами без встроенной ОС c) Специализированными аппаратными устройствами со встроенной ОС, только программная реализация невозможна d) Аппаратно-программными устройствами	ОПК-9

97.	a	Механизм безопасности – это a) Программное и/или аппаратное средство, которое определяет и/или предотвращает атаку b) Настройки межсетевого экрана c) Настройки программного обеспечения d) Аппаратура, которая предотвращает несанкционированный доступ к файлам и программам	ОПК-9
98.	a	Узел ESXI добавлен в vCenter Server, но не отвечает в vSphere Web Client. Какой порт должен быть открыть в брандмауэре a) порт 902 (UDP) b) порт 443 (TCP) c) порт 903 (TCP) d) все перечисленные	ОПК-9
99.	a	Недостатки межсетевых экранов прикладного уровня a) Производительность межсетевого экрана прикладного уровня ниже, чем у пакетного фильтра b) Межсетевой экран прикладного уровня обязательно разрывает TCP-соединение c) Межсетевой экран прикладного уровня не может анализировать заголовки транспортного и сетевого уровней d) Межсетевой экран прикладного уровня обеспечивает меньший уровень безопасности, чем пакетный фильтр	ОПК-9
100.	b	Понятие сессии в NAT a) Трансляция адресов, выполняемая NAT, не использует понятие на сессии. Каждый входящий и исходящий пакет преобразуется по своим правилам b) Трансляция адресов, выполняемая NAT, использует понятие сессии и единообразным образом преобразует входящие и исходящие пакеты, принадлежащих одной и той же сессии c) Трансляция адресов, выполняемая NAT, использует понятие сессии, но каждый входящий и исходящий пакет преобразуется по своим правилам d) Трансляция адресов, выполняемая NAT, не использует понятие сессии. Все входящие и исходящие пакеты преобразуются единообразным образом	ОПК-9

101.	c	В сети демилитаризованной зоны (DMZ) должны располагаться a) Рабочие станции пользователей b) Серверы, которые должны быть доступны только внутренним пользователям c) Серверы, которые должны быть доступны из внешних сетей d) Серверы, содержащие наиболее чувствительные данные	ОПК-9
102.	A, b, c, d	Компоненты IDS a) Сенсор или агент b) Управляющий сервер c) Сервер базы данных d) Консоль администрирования	ОПК-9
103.	A, b, d	Источники данных, используемые системами host-based анализа уязвимостей a) Параметры конфигурации b) Системные атрибуты c) Внутренние параметры состояния системы d) Открытые параметры состояния системы	ОПК-9
104.	a	Проверка доступности IP-адреса источника с входящего интерфейса выполняется следующим образом a) Ищется соответствие параметров пакета с правилами доступа (Access Rules) b) Ищется соответствие параметров пакета с правилами фильтрования (IP Rules) c) Ищется соответствие параметров пакета с параметрами Ethernet-интерфейсов d) Ищется соответствие параметров пакета с параметрами vlan-интерфейсов	ОПК-9
105.	A, c	К требованиям, которые накладывает внешнее окружение на функционирование межсетевого экрана, относятся a) Используемые транспортные протоколы (IPv4 или IPv6) b) Количество отделов в организации c) Специфика защищаемых сервисов d) Количество комнат в помещении	ОПК-9
106.	A, b	Причины, по которым необходимо создавать «оборону в глубину»	ОПК-9

		a) Ни один из сервисов безопасности не может гарантировать 100%-ную защиту + b) Сбой единственного используемого сервиса безопасности не должен означать, что нарушитель получает полный доступ в систему c) Межсетевой экран не может быть конечной точкой VPN d) Межсетевой экран не может выполнять аутентификацию пользователей	
107.	d	Прокси-шлюзов прикладного уровня a) Изменяют IP-адрес источника на IP-адрес своего интерфейса b) Изменяют MAC-адрес источника на MAC-адрес своего интерфейса c) Изменяют номер порта источника d) Создают два отдельных соединения – одно между клиентом и прокси-агентом, другое – между прокси-агентом и реальным сервером	ОПК-9
108.	d	На границе сетевого периметра a) Должен блокироваться исходящий трафик, если у него IP-адрес источника принадлежит внутренней сети b) Должен блокироваться входящий трафик, если у него IP-адрес источника не принадлежит внутренней сети c) Должен блокироваться весь входящий трафик d) Должен блокироваться входящий трафик, если у него IP-адрес источника принадлежит внутренней сети	ОПК-9
109.	a	Выберите наиболее оптимальное окружение межсетевого экрана a) Конечные точки VPN совмещены с межсетевым экраном b) Конечные точки VPN расположены за межсетевым экраном c) Конечные точки VPN и межсетевой экран расположены в разных точках входа в локальную сеть d) Конечные точки VPN расположены перед межсетевым экраном	ОПК-9

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется, если студент показал глубокое, прочное и аргументированное освоение программного учебного материала, при этом поставленный вопрос раскрыт последовательно, четко и логически стройно, в полном исчерпывающем объеме, основные категории, понятия и термины учебного курса формулировались правильно, не допущено при ответе ошибок

Оценка «хорошо» выставляется, если студент показал твердое знание программного учебного материала, при этом поставленный вопрос раскрыт грамотно и по существу, в достаточно полном объеме, основные категории, понятия и термины учебного курса формулировались правильно, допущены при ответе отдельные неточности или одна ошибка;

Оценка «удовлетворительно» выставляется, если студент показал знание только основной части учебного материала без его частных деталей, при этом поставленный вопрос раскрыт с нарушением логической последовательности, не в полном объеме, были допущены неточные формулировки основных категорий, понятий и терминов учебного курса, а также ошибки (не более двух) или ряд незначительных неточностей, не исказивших существенно суть ответа;

Оценка «неудовлетворительно» выставляется, студенту, который не знает значительной части программного материала, допускает грубые ошибки (более двух), существенно исказившие его суть. Оценка неудовлетворительно выставляется также, если отсутствует письменный ответ на вопрос, либо студент отказался его сдавать.

**** в соответствии с результатами освоения дисциплины и видами заданий***