МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

УТВЕРЖДАЮ
Зам. директора по учебной работе
ИСТиД (филиал) СКФУ в г. Пятигорске
_____ М.В. Мартыненко
«__» _____ 20_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность информационных систем

Направление подготовки	09.03.02 Информационные системы и технологии
Профиль подготовки	Информационные системы и технологии
Квалификация выпускника	Бакалавр
Форма обучения	очная
Год начала обучения	2020
Изучается в	7 семестре

СОГЛАСОВАНО:
Зав. кафедрой СУиИТ
_____ И.М. Першин
«__» _____ 20_ г.

Рассмотрено УМК
Протокол №___ от «___»_____

Председатель УМК института
_____ А.Б. Нарыжная

РАЗРАБОТАНО:
Зав. кафедрой СУиИТ
_____ И.М. Першин
«__» _____ 20_г.

Доцент кафедры СУиИТ
_____ Т.И. Дровосекова
«__» _____ 20_ г.

Пятигорск, 2020

1. Цели и задачи освоения дисциплины

Цели дисциплины:

- Поэтапное формирование у студентов следующих знаний, умений и владений: об основах информационной безопасности;
- о проблемах безопасности;
- об основных методах защиты информации в информационных системах;
- об основных методах защиты информации в ПК;
- об основных методах защиты информации в компьютерных сетях;
- об основных методах криптографической защиты информации;
- о правовых основах защиты информации.

Изучение дисциплины ставит перед собой задачи:

- ознакомить студентов с общими проблемами безопасности;
- ознакомить с угрозами безопасности информации;
- дать сведения о способах и средствах добывания информации;
- дать сведения о способах и средствах противодействия утечки информации;
- ознакомить с методами защиты информации в компьютерных сетях;
- ознакомить с компьютерными вирусами;
- ознакомить с антивирусными программами.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность информационных систем» относится к обязательной части дисциплин блока Б1 ОП ВО подготовки бакалавра направления 09.03.02 Информационные системы и технологии. Её освоение проходит в 7 семестре.

3.Связь с предшествующими дисциплинами

Успешному освоению данной дисциплины способствуют знания, полученные при предшествующем изучении дисциплины Цифровая грамотность и обработка больших данных.

4.Связь с последующими дисциплинами

Знания, умения и навыки, приобретенные студентом при изучении дисциплины являются базовыми для освоения таких курсов как: Предметно-ориентированные информационные системы, Надежность информационных систем.

5.Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

5.1 Наименование компетенции

Код	Формулировка:

ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

5.2 Знания, умения и (или) опыт деятельности, характеризующие этапы формирования компетенций

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	ОПК-3

6. Объем учебной дисциплины

Объем занятий: Итого	135 ч.	5 з.е.
В т.ч. аудиторных	40,5 ч.	
Из них:		
Лекций	13,5 ч.	
Лабораторных занятий	27ч.	
Самостоятельная работа	94,5 ч.	

Зачет с оценкой 7 семестр

7. Содержание дисциплины. Структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов занятий

7.1 Тематический план дисциплины

№	Раздел (тема) дисциплины	Реализуемые компетенции	Контактная работа обучающихся с	Са мос тоя тел

			преподавателем, часов				
			Лекции	**Практические занятия**	**Лабораторные работы**	**Групповые консультации**	
7 семестр							
1.	**Тема 1.** Основы сетевых технологий и обеспечение безопасности информационных систем	ОПК-3	1,5			0	10
2.	**Тема 2.** Возможные уязвимости, угрозы и атаки на информационные системы	ОПК-3	1,5			0	5
3.	**Тема 3.** Классификация атак по уровням иерархической модели OSI.	ОПК-3	1,5			0	5
4.	**Тема 4.** Мониторинг и анализ трафика в сети.	ОПК-3	1,5			0	5
5.	**Тема 5.** Атаки на беспроводные устройства и защита от них.	ОПК-3	1,5			0	5
6.	**Тема 6.** Основные типы уязвимостей информационных систем. Защита от уязвимостей.	ОПК-3	1,5			0	5
7.	**Тема 7.** Атаки в виртуальной среде и защита от них.	ОПК-3	1,5			0	5
8.	**Тема 8.** Межсетевые экраны. Изучение принципов работы межсетевых экранов	ОПК-3	1,5		3	0	5
9.	**Тема 9.** Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения вторжений.	ОПК-3	1,5		3	0	5

10.	**Тема 10.** Базовое администрирование и разрешение сетевых проблем с использованием утилит командной строки Windows.	ОПК-3			3	0	5
11.	**Тема11.** Анализ и изучение заголовков различных сетевых пакетов.	ОПК-3			3	0	5
12.	**Тема 12.** Сканирование и исследования безопасности сети с помощью сканера Nmap.	ОПК-3			3	0	5
13.	**Тема 13.** Методы анализа сетевого трафика с использованием WireShark.	ОПК-3			3	0	5
14.	**Тема 14.** Установка и настройка VPN сервера.	ОПК-3			1,5	0	5
15.	**Тема 15.** Применение криптографии для безопасности данных. Использование криптостем PGP TrueCrypt.	ОПК-3			1,5	0	5
16.	**Тема 16.** Проверка безопасности хоста, выявление ошибок конфигурации. Microsoft Baseline Security.	ОПК-3			1,5	0	5
17.	**Тема 17.** Системы разграничения доступа.	ОПК-3			1,5	0	5
18.	**Тема 18.** Управление доступом.	ОПК-3			1,5	0	4,5
19.	**Тема 19.** Аудит и журналы безопасности.	ОПК-3			1,5		
	Итого за 7 семестр		**13,5**		**27**		**94,5**
	Итого		**13,5**		**27**		**94,5**

7.2 Наименование и содержание лекций

№ Темы	**Наименование тем дисциплины, их краткое содержание**	**Обьем часов**	**Интерактивная форма проведения**

	7 семестр		
1	**Тема 1. Основы сетевых технологий и обеспечение безопасности информационных систем.** Особенности и области применения систем контроля версий. История развития программного обеспечения для контроля версий. Локальные системы контроля версий. Централизованные системы контроля версий. Децентрализованные системы контроля версий.	1,5	
2	**Тема 2. Возможные уязвимости, угрозы и атаки на информационные системы.** Угроза, уязвимость, атака. Классификация уязвимостей, Источники возникновения уязвимостей, Классификация уязвимостей по уровню в инфраструктуре АС, Классификация уязвимостей по степени риска, CommonVulnera bilitiesand Exposures, Классификация атак по целям, Классификация атак по мотивации действий, Местонахождение нарушителя, Механизмы реализации атак, Статистика по уязвимостям и атакам, Примеры атак.	1,5	
3	**Тема 3. Классификация атак по уровням иерархической модели OSI.** Уровни модели OSI. Фрагментация данных. Атака Pingflooding. Нестандартные протоколы, инкапсулированные в IP. Атака smurf. Атака DNS spoofing. Атака IP spoofing. Навязывание пакетов. Sniffing — прослушивание канала. Перехват пакетов на маршрутизаторе. Навязывание хосту ложного маршрута с помощью протокола ICMP. WinNuke. Подмена доверенного хоста. Технологии обнаружения атак.	1,5	
4	**Тема 4. Мониторинг и анализ трафика в сети.** Обзор методов анализа и мониторинга сетевого трафика. Важность мониторинга и анализа сети. Способы мониторинга и анализа. Методы мониторинга, основанные на маршрутизаторе. Протокол простого сетевого мониторинга, Удалённый мониторинг, Netflow, Технологии не основанные на маршрутизаторах, Активный мониторинг, Пассивный мониторинг, Комбинированный мониторинг, Просмотр ресурсов на концах сети, Сетевой монитор с собственной конфигурацией, Атакуемые сетевые компоненты: Сервера, Рабочие станции, Среда передачи информации, Узлы коммутации сетей.	1,5	
5	**Тема 5. Атаки на беспроводные устройства и защита от них.** Организация сетей Wi-Fi . Угрозы. Прямые угрозы. Чужаки. Нефиксированная природа связи. Уязвимости сетей и устройств. Некорректно	1,5	

	сконфигурированные точки доступа. 2.1.3.2 Некорректно сконфигурированные беспроводные клиенты. Взлом шифрования. Имперсонация и Identity Theft. Отказы в обслуживании. Косвенные угрозы. Утечки информации из проводной сети. Особенности функционирования беспроводных сетей. Методы ограничения доступа. Методы аутентификации . Методы шифрования. Атаки на сети wi-fi.		
6	**Тема 6. Основные типы уязвимостей информационных систем. Защита от уязвимостей.** Классификация уязвимостей: технологические, организационные, эксплуатационные. Типовые уязвимости: Неподдерживаемые версии операционных систем и системного программного обеспечения, Уязвимости веб-серверов, Использование небезопасных протоколов управления, Использование небезопасных протоколов SSL и TLS, Слабые пароли WPA/WPA2-PSK, Использование протокола разрешения имен NetBIOS по TCP/IP, Межсайтовый скриптинг. Устранение выявленных уязвимостей.	1,5	
7	**Тема 7. Атаки в виртуальной среде и защита от них.** Разведка. Атаки на сети с WEP-шифрованием. Пассивные сетевые атаки. Активные сетевые атаки. Повторное использование вектора инициализации (Initialization Vector Replay Attacks). Манипуляция битами (Bit-Flipping Attacks). Атаки на сети с WPA/WPA2-шифрованием. Атака по словарю на WPA/WPA2 PSK. Атака переустановки ключа в WPA и WPA2 (KRACK)	1,5	
8	**Тема 8. Межсетевые экраны. Изучение принципов работы межсетевых экранов** Методы анализа сетевой информации, Статистический метод, Экспертные системы, Нейронные сети. Межсетевые экраны: Назначение, История, Фильтрация трафика, Классификация межсетевых экранов, Управляемые коммутаторы, Пакетные фильтры, Шлюзы сеансового уровня, Посредники прикладного уровня, Инспекторы состояния, Реализация, Ограниченность анализа межсетевого экрана.	1,5	
9	**Тема 9. Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения**	1,5	

	вторжений. Система обнаружения вторжений, Виды систем обнаружения вторжений, Пассивные и активные системы обнаружения вторжений, Сравнение СОВ и межсетевого экрана, История разработок СОВ.		
	Итого за 7 семестр	**13,5**	**-**
	Итого	**13,5**	**-**

7.3 Наименование лабораторных работ

№ Темы	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактивная форма проведения
	7 семестр		
Тема 8. Межсетевые экраны. Изучение принципов работы межсетевых экранов			
1	Изучение принципов работы межсетевых экранов. Изучение и конфигурирование межсетевого экрана Windows. Классификация. Профиль брандмауэра – домен, частный, общий. Состояние брандмауэра. Правила для исходящих и входящих соединений. Мастер создания правила для нового исходящего подключения.	3	
Тема 9. Системы обнаружения и предупреждения вторжений. Установка и конфигурирование системы обнаружения вторжений.			
2.	Понятие и основные функции системы обнаружения вторжений. Установка Snort. Настройка в режим IDS. Создание пользователя. Конфигурационные файлы и файлы настроек. Установка Barnyard2 для снижения нагрузки на сервер. Установка и настройка PulledPork для задания правил для Snort. Установка BasicAnalysisandSecurityEngine – графического визуализатора. Создание службы из Snort и Barnyard2. Отслеживание действия в сети. Создание своих правил в Snort.	3	
Тема 10. Базовое администрирование и разрешение сетевых проблем с использованием утилит командной строки Windows.			
3.	Использование базовых команд командной строки windows, применяемых для поиска проблем в сети. Проверка настроек IP. проверка соединения на уровне протоколаIP с использованием команды Ping. Определение маршрута (трассировка) пакетов с использованием команды tracert. Разрешение доменных имен с использованием команды nslookup. Проверка вашей сетевой конфигурации и сетевой статистики командой netstat.	3	
Тема11. Анализ и изучение заголовков различных сетевых пакетов.			
4.	Анализ различных пакетов такие как TCP, HTTP,	3	

	ICMP, DNS с использованием Wireshark. Установка Wireshark. Файл с захваченным трафиком. Исследование заголовка ARP. Исследование заголовка TCP. Исследование заголовка HTTP. Исследование заголовка ICMP. Исследование заголовка DNS. Исследование заголовка UDP.		
Тема 12. Сканирование и исследования безопасности сети с помощью сканера Nmap.			
5.	Изучение и практическое применение утилиты для сканирования и исследования безопасности сети Nmap и графической оболочки Zenmap. Получение списка открытых портов. Определение операционной системы. Определение адресов активных хостов без сканирования портов. Сканирование хостов разными методами. Определение наличия сетевого экрана. Выбор оптимальных методов сканирования портов с целью избежать обнаружения.	3	
Тема 13. Методы анализа сетевого трафика с использованием WireShark.			
6.	Захват пакетов. Особенности и области применения WireShark. Неразборчивый режим сетевой карты. Основные элементы интерфейса программы Wireshark. Условия фильтрации трафика, их задание. Объединение условий фильтрации. Отслеживание соединения. Извлечение файлов из перехваченного трафика. Определение протоколов, используемых в перехваченном трафике.	3	
Тема 14. Установка и настройка VPN сервера.			
7.	Виртуальная частная сеть. Типы VPN-соединений. Назначение VPN-сервера. Конфигурация виртуальных машин. Конфигурация шлюза. Конфигурация клиента. Установка VPN-Server. Базовая конфигурация VPN-сервера. Настройка NAT и DHCP. Установка VPN-клиента.	1,5	
Тема 15. Применение криптографии для безопасности данных. Использование криптостем PGP TrueCrypt.			
8.	Программы для шифрования информации и создания электронных цифровых подписей. Программы для шифрования сообщений с использованием асимметричных пар ключей, генерируемых пользователями. Установка VeraCrypt. Локализация. Создание зашифрованногоконтейнера. Подключение и отключение контейнера. Криптосистема PGP. Установка GnuPG. Генерация пары ключей и импорт ключей. Шифрование, расшифровка и цифровая подпись с использованием своей пары ключей. Использование цифровой подписи. Импорт чужого публичного ключа. Проверка подписи документа с использованием чужого публичного ключа. Шифрование документа с использованием чужого публичного ключа. Импорт чужого приватного ключа.	1,5	
Тема 16. Проверка безопасности хоста, выявление ошибок конфигурации. Microsoft Baseline Security.			
9.	Автоматическое сканирование по заданным шаблонам. Проверка продуктов Microsoft на наличие уязвимостей – Microsot Baseline Security Analyzer. Составление сценария сканирования по определенным требованиям. Автоматизация проверки.	1,5	

Тема 17. Системы разграничения доступа.			
10	Дискреционная политика безопасности; мандатная политика безопасности; субъект доступа; объект доступа; виды доступа; монитор обращений; монитор безопасности объектов; домен безопасности; реестр операционной системы; контроль целостности объектов; ключ симметричного шифрования; ключи асимметричного шифрования.	1,5	
Тема 18. Управление доступом.			
11	Учетные записи пользователей и компьютеров; Управление пользователями ; Управление группами ; управление компьютерами.	1,5	
Тема 19. Аудит и журналы безопасности.			
12	Роль аудита в обеспечении безопасности компьютерной системы; формирование информации о событиях аудита, информация, которая может быть получена в результате аудита, типы аудита, активизация политики аудита, применение политики аудита для выбранных объектов и пользователей, использование журналов безопасности, право на настройку аудита и проверку результатов аудитаю	1,5	
	Итого 7 семестр	**27**	
	Итого	**27**	

7.4 Наименование практических занятий

Не предусмотрены учебным планом.

7.4 Технологическая карта самостоятельной работы обучающегося

Код реализуемой компетенции	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОПК-3	Самостоятельное изучение литературы по темам № 1 - 9	Конспект	Собеседование	77,76	8,64	86,4
ОПК-3	Подготовки к лабораторным занятиям	*Решение проблемных задач*	Отчет письменный	7,29	0,81	8,1
Итого за 7 семестр				85,05	9,45	94,5
Итого				85,05	9,45	94,5

8 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО. Паспорт фонда оценочных средств

Код оцениваемой компетенции (или её части)	Этап формирования компетенции (№ темы)	Средства и технологии оценки	Тип контроля	Вид контроля	Наименование оценочного средства
ОПК-3	1-9	Собеседование	Текущий	устный	Вопросы для собеседования
ОПК-3	6, 8	Решение разноуровневых задач	Текущий	письменный с помощью технических средств	Темы индивидуальных заданий по лабораторным работам

8.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровни сформированности компетенций	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов
ОПК-3					
Базовый	Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	*Не знает:* принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*Знает недостаточно хорошо:* принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*Знает достаточно хорошо:* принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
	Уметь: решать	*Не умеет:*	*Умеет*	*Умеет*	

	стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*недостаточно хорошо:* решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*достаточно хорошо:* решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
	Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	*Не владеет:* навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	*Владеет недостаточно хорошо:* навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	*Владеет достаточно хорошо:* навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	
Повышенный	**Знает отлично:** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно				**Знает отлично:** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры

	- коммуникационных технологий и с учетом основных требований информационной безопасности				с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	Умеет: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности				*Умеет на отлично:* решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности				*Владеет в полном объеме:* навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине

оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
1.	Собеседование по темам	5-ая неделя	15
2.	Лабораторные работы 1-7	7-ая неделя	15
3.	Лабораторные работы 8-12	12 –ая неделя	25
	Итого за 7 семестр		**55**
	Итого		**55**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

Промежуточная аттестация

Промежуточная аттестация в форме **зачета с оценкой.**

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет ($S_{зач}$) при различных рейтинговых баллах по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине по результатам работы в семестре ($R_{сем}$)	**Количество баллов за зачет ($S_{зач}$)**
$50 \le R_{сем} \le 60$	**40**
$39 \le R_{сем} < 50$	**35**
$33 \le R_{сем} < 39$	**27**
$R_{сем} < 33$	**0**

При дифференцированном зачете используется шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе

Шкала пересчета рейтингового балла по дисциплине
в оценку по 5-балльной системе

Рейтинговый балл по дисциплине	***Оценка по 5-балльной системе***
88 – 100	*Отлично*
72 – 87	*Хорошо*
53 – 71	*Удовлетворительно*
< 53	*Неудовлетворительно*

8.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций для проведения промежуточной аттестации

Процедура зачета с оценкой как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

8.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Текущая аттестация студентов проводится преподавателем, ведущим лекционные и лабораторные занятия по дисциплине. К лабораторному занятию студент должен подготовить ответы на вопросы, выполнить задания по теме занятия. Максимальное количество баллов студент получает, если он активно участвует в работе, владеет материалом, умеет логично и четко излагать мысли, творчески подходит к решению основных вопросов темы, показывает самостоятельность мышления.

Основанием для снижением оценки являются:

- слабое знание темы и основной терминологии;
- пассивность участия в групповой работе;
- отсутствие умения применить теоретические знания для решения практических задач;
- несвоевременность предоставления выполненных работ.

Критерии оценивания индивидуальных заданий, собеседования приведены в Фонде оценочных средств по дисциплине «Безопасность информационных систем».

9 Методические указания для обучающихся по освоению дисциплины

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, использую рекомендуемые источники информации:

№ п/п	Вид самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополни-тельная	Методи-ческая	Интернет-ресурсы
1	Самостоятельное изучение литературы	1-4	1-4	1-2	1-4

2	Подготовка к лабораторным занятиям	1-4	1-4	1-2	1-4

10.1.1.Перечень основной литературы:

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 c.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
3. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с.
4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Флинта, 2016. - 224 с.

10.1.2. Перечень дополнительной литературы:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. : [учебник] / В.Г. Олифер, Н.А. Олифер. - 4-е изд. - СПб. : Питер, 2011. - 944 с.
2. Таненбаум, Э. Компьютерные сети : [учеб. пособие] / Э. Таненбаум ; пер. с англ. В. Шрага. - 4-е изд. - СПб. : Питер, 2007. - 992 с. .
3. Сети и телекоммуникации : учеб. пособие / Б.В. Соболь, А.А. Манин, М.С. Герасименко. - Ростов н/Д : Феникс, 2015. - 191 с. .
4. Галицкий, А. В. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. - М. : ДМК Пресс, 2004. - 616 с.

10.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Безопасность ИС»
2. Методические указания по выполнению лабораторных работ по дисциплине «Безопасность ИС»

10.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://www.biblioclub.ru/ - электронная библиотека
2. http://www.uts-edu.ru/ - «Электронные курсы»
3. http://www.intuit.ru - Национальный открытый университет «ИНТУИТ»;
4. http://www.window.edu.ru - Единое окно доступа к образовательным ресурсам.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включа перечень программного обеспечения и информационных справочных систем

Базовый пакет программ Microsoft Office Standard 2013. Бессрочная лицензия. Дата окончания срока поддержки (обновления) 11.04.2023г., Microsoft Windows Профессиональная. Бессрочная лицензия. Дата окончания срока поддержки (обновления) 10.01.2023г., Oracle VM VirtualBox (бесплатный), Wireshark (бесплатный),SoftEther VPN

Server (бесплатный),Gnu Privacy Guard (бесплатный), VeraCript (бесплатный), Microsoft Baseline Security (бесплатный), Snort 2.9.12 (бесплатный), Ubuntu 16 (бесплатный)

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Учебная аудитория для проведения занятий лекционного типа: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, Мультимедиа проектор, магнитно-маркерная доска. Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин.

2. Учебная аудитория для проведения занятий семинарского типа (лабораторных работ): Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, Мультимедиа проектор, магнитно-маркерная доска.

3. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, Мультимедиа проектор, магнитно-маркерная доска.