Приложение
к рабочей программе модуля

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Код модуля	**Модуль**
М.1.18	Техническое обеспечение национальной безопасности

Екатеринбург, 2019

Фонд оценочных средств по модулю составлен авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Лучинин Александр Сергеевич	к.т.н. доцент	доцент	Департамент радиоэлектроники и связи
2	Виноградова Нина Сергеевна		ст. преподаватель	Департамент радиоэлектроники и связи
3	Белоусова Вероника Игоревна	к.ф.-м.н	доцент	Департамент информационных технологий и автоматики

Дирекция образовательных программ Р. Х. Токарева

1. СТРУКТУРА И ОБЪЕМ МОДУЛЯ Техническое обеспечение национальной безопасности

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах	Форма итоговой промежуточной аттестации по дисциплинам модуля и в целом по модулю
1.	Администрирование информационных систем	3/108	зачет
2	Безопасность и защита веб-приложений	3/108	зачет
3	Техническая защита информации	3/108	зачет
	ИТОГО по модулю:	9/324	Не предусмотрено

2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО МОДУЛЮ

2.1. Проект по модулю

Не предусмотрено.

2.2. Интегрированный экзамен по модулю

Не предусмотрено.

РАЗДЕЛ 3
ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО МОДУЛЮ
ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 1
АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Фонд оценочных средств составлен автором(ами):

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Лучинин Александр Сергеевич	к.т.н. доцент	доцент	Департамент радиоэлектроники и связи
2	Виноградова Нина Сергеевна		ст. преподаватель	Департамент радиоэлектроники и связи

Рекомендовано учебно-методическим советом института государственного управления и предпринимательства

Протокол № 10 от 26 июня 2019г.

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ «АНАЛИЗ БОЛЬШИХ ДАННЫХ» И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации.

Таблица 1.

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
1	**2**
ПК-8 Способен соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности	**Знать:** - основные сведения о формировании и функционированию служб управления; - вопросы обеспечения информационной безопасности и функционирования информационных систем администрирования; - функции и обязанности принятия управленческих решений администратора сети в вопросах предотвращения и нейтрализации угроз функционирования информационных систем. **Уметь:** - работать с программными средствами общего назначения, искать информацию с применением правил поиска (построения запросов) в базах данных, компьютерных сетях нормативно-справочной информации; **Практический опыт, владение:** - знаниями информационных систем управления и методами информационных процессов и технологий принятия управленческих решений для функционирования информационных систем управления согласно требованием к программному обеспечению различных уровней административного управления. - навыками практического использования современного программного обеспечения и вычислительной техники и периферийных устройств.
ПК-10. Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности	**Знать:** - основы законодательного регулирования деятельности информационных систем - основы управления информационными системами **Уметь:** - анализировать эффективность информационных систем в профессиональной сфере **Практический опыт, владение:** - базовыми навыками администрирования информационных систем

2.ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

2.1.Распределение объема времени по видам учебной работы

Таблица 2.

№ п/п	Наименования дисциплины модуля	**Объем времени, отведенный на освоение дисциплины модуля** *6 з.е.*								
		Аудиторные занятия, час.				**Промежуточная аттестация** (форма итогового контроля /час.)	**Контактная работа (час.)**	**Самостоятельная работа студента, включая текущую аттестацию, час.**	**Всего по дисциплине**	
		Занятия лекционного типа	**Практические занятия**	**Лабораторные работы**	**Всего**				**Час.**	**Зач. ед.**
1.	*Администрирование информационных систем*	*17*	*34*	*-*	*51*	*зачет/4*	*58,9*	*57*	*108*	*3*
Всего на освоение дисциплины модуля (час.)		*17*	*34*	*-*	*51*	*зачет/4*	*58,9*	*57*	*108*	*3*
								Итого по модулю:	**108**	**3**

2.2.Виды, количество и объем времени на СРС по дисциплине*

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество мероприятий СРС	Объем СРС (час.)
1.	*Подготовка к лекциям*		*3 час.*
2	*Подготовка к практическим занятиям*		*30 час.*
3	*Подготовка к контрольной работе*	*1*	*8 час.*
4	*Выполнение домашней работы*	*1*	*12 час*
5	*Подготовка к зачету*	*1*	*4 час.*
Итого на СРС по дисциплине:			*57 час.*

** Объем времени на СРС по дисциплине не должен превышать объем времени на самостоятельную работу студента, включая текущую аттестацию, указанный в табл. 2*

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине
Семестр 7

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лекций	*семестр 7*	*20*
Участие в работе на лекциях	*семестр 7*	*30*
Контрольная работа	*семестр 7*	*50*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 1		
Промежуточная аттестация по лекциям – нет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,5		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение практических/семинарских занятий	*семестр 7*	25
Домашняя работа	*семестр 7*	75
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0,5		
Промежуточная аттестация по практическим/семинарским занятиям–*зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0,5**		

3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –нет

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Не предусмотрено		
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – …		

3.3. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	Коэффициент значимости результатов освоения дисциплины в семестре
Семестр 7	1

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1.В рамках БРС применяются утвержденные на кафедре критерии (признаки) оценивания достижений студентов на соответствие указанным в табл.1 ФОС индикаторам в рамках контрольно-оценочного мероприятия по дисциплине модуля (табл.4).

Таблица 4

Критерии оценивания результатов обучения

Результаты обучения	Критерии оценивания результатов обучения на соответствие индикаторам
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2. Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5.

Шкала оценивания результатов обучения по уровням

Характеристика уровней освоения результатов обучения			
№ п/п	Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	Шкала оценивания	
		Традиционная характеристика уровня	Качественная характеристика уровня

1.	Результаты обучения освоены и в полном объеме соответствуют индикаторам, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения освоены и соответствуют индикаторам, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Освоение результатов обучения не в полной мере соответствует индикаторам, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ МОДУЛЯ

Задания по контрольно-оценочным мероприятиям должны обеспечивать освоение результатов обучения и предметного содержания дисциплины и достижение индикаторов на соответствующем уровне.

5.1. Описание оценочных материалов текущего контроля по дисциплине модуля

5.1.1. Практические занятия

Номер занятия	Темы практических занятий	Время на проведение занятия (час.)
1	Информационные системы и их типы. Задачи, функции и виды администрирования в информационных системах	2
2	Понятие компьютерной сети. Локальные и глобальные сети. Классификация локальных сетей. Основные компоненты сети	2
3	Технологии хранения и способы их реализации. Типы DAS. Преимущества и недостатки DAS, NAS, SAN.Основной и динамический диски. Управление дисками и томами. Выбор файловой системы. Реализация и принцип работы RAID. Уровни RAID	4
4	Функциональные возможности и эффективность реализации системы Windows Server. Выпуски Windows Server. Методы, типы и этапы установки Windows Server. Параметры конфигурации после установки Windows Server.	4

5	Реализация роли Hyper-V. Виртуальные жесткие диски. Виртуальные сети и программный коммутатор в Hyper-V. Настройка и управление виртуальными машинами.	2
6	Архитектура стека протоколов TCP/IP. Модель OSI. Стек OSI. Модель TCP/IP. Стек TCP/IP. Структура TCP/IP.	4
7	IP-адресация и маршрутизация. Адресация в TCP/IP-сетях. Типы адресов стека TCP/IP. Структура IP-адреса. Классы IP-адресов. Особые IP-адреса. Протоколы IPv6 и ARP.	2
8	Система доменных имен. Служба DNS. Процесс разрешения имен.	2
9	Управление пользователями, группами и компьютерами. Реализация подразделений. Групповые политики. Создание объектов групповой политики и управление ими.	4
10	Обзор модели многоуровневой защиты. Безопасность на физическом уровне. Безопасность в Интернете. Средства сетевой безопасности Windows Server.	2
11	Функции шифрования данных. Шифрованная файловая система (EFS). Цифровые сертификаты. Типы брандмауэров. Защита электронной почты.	4
12	Обеспечение безопасности сервера.	2
	Всего:	34

5.1.2. Лабораторные занятия

Не предусмотрено

5.1.3. Курсовая работа / Курсовой проект

Не предусмотрено

5.1.4. Контрольная работа

Примерная тематика контрольной работы

1. Основные этапы и процессы администрирования информационных систем.
2. Необходимость защиты информационных систем и телекоммуникаций
3. Основные методы и средства администрирования информационных систем.
4. Многоуровневая модель OSI.
5. Стандарты Интернета.
6. Основы коммутации и маршрутизации в IP-сетях.
7. Маршрутизаторы. Алгоритмы маршрутизации.
8. Сетевые функции операционных систем семейства MS Windows, их особенности.
9. Инструменты управления и обслуживания сети.
10. Разграничение доступа к данным. Управление безопасностью общих сетевых ресурсов.
11. Службы каталогов, их функции и назначение.
12. Доменная модель службы каталогов. Иерархия доменов.
13. Инструменты управления объектами службы каталогов в Windows Server.
14. Сетевые и персональные операционные системы (ОС).
15. Методы обеспечения безопасности аутентификации пользователей в распределенных системах, схема Kerberos.

16. Разграничение доступа к файлам и каталогам.
17. Аудит информационной системы.
18. Автоматизация административных задач.
19. Администрирование баз данных
20. Архитектура вычислительной среды.
21. Структура MS SQL Server.
22. Обеспечение надежности БД.
23. Архитектура построения распределенных информационных систем.
24. Информационные службы Интернет
25. Почтовые серверы, их администрирование
26. Безопасность информационных служб в сети Интернет
27. Организация доступа в Интернет.
28. Электронные службы.
29. Аудит/контроль использования ресурсов.
30. Процесс движения пакетов в сети. Фрагментация пакета. Время жизни пакета.
31. Сетевые маски. Организация подсетей.
32. Система доменных имен.
33. Протоколы маршрутизации.
34. Процедура установления соединения. Передача данных в рамках установленного соединения.
35. Инструменты управления и обслуживания сети.
36. Управление файловым сервером. Контроль доступности файловых ресурсов.
37. Служба каталогов Active Directory.
38. Сайты, межсайтовые соединения.
39. Клиент-серверные и одноранговые ОС.
40. Сетевые и распределенные файловые системы.
41. Политики учетных записей.
42. Локальные и распределенные СУБД.
43. Физическая и логическая структура БД.
44. Копирование и журнализация.
45. Инструменты разграничения доступа к данным.
46. Основные веб-сервисы, их применение в информационных системах.
47. Интернет, построение распределенной сети предприятия.
48. Параметры настройки веб-сервера.
49. Управление доступом к веб-ресурсам, средства аутентификации пользователей, анонимный доступ.
50. Статические и динамические страницы, разрешения на выполнение сценариев и приложений.
51. Почтовые службы, их функции и назначение. Примеры почтовых серверов.
52. Аутентификация в распределенных системах.
53. Организация доступа в Интернет. Коммутируемый доступ. Выделенные линии.
54. Методы оценивания стоимости коммуникаций.
55. Удаленное управление компьютером

5.1.5. Домашняя работа

1. Понятие «администрирование» применительно к информационным системам.
2. Информационные системы и их типы. Задачи, функции и виды администрирования в информационных системах
3. Автоматизация управления сетью. Администрирование в корпоративных сетях.
4. Инфраструктура ИТ.
5. Понятие компьютерной сети.
6. Локальные и глобальные сети. Классификация локальных сетей.

7. Основные компоненты сети. Сетевые устройства.
8. Топология сети.
9. Типы кабельных сред передачи данных.
10. Пакеты и протоколы.
11. Технологии хранения и способы их реализации.
12. Типы DAS. Преимущества и недостатки DAS, NAS, SAN.
13. Основной и динамический диски. Управление дисками и томами.
14. Выбор файловой системы.
15. Реализация и принцип работы RAID.
16. Уровни RAID.
17. Функциональные возможности и эффективность реализации системы Windows Server. Выпуски Windows Server
18. Методы, типы и этапы установки Windows Server.
19. Параметры конфигурации после установки Windows Server.
20. Развертывание роли сервера в соответствии с определенными бизнес-сценариями. Реализация соответствующих ролей сервера для поддержки конкретного сценария.
21. Обзор технологий виртуализации.
22. Управление виртуализацией. Реализация роли Hyper-V.
23. Виртуальные жесткие диски. Виртуальные сети и программный коммутатор в Hyper-V. Настройка и управление виртуальными машинами.
24. Основные возможности диспетчера виртуальных машин VMM 2008.
25. Модель OSI. Стек OSI.
26. Модель TCP/IP. Стек TCP/IP. Структура TCP/IP.
27. Обзор основных протоколов.
28. Утилиты диагностики TCP/IP

5.1.6. Расчетная работа / Расчетно-графическая работа

Не предусмотрено

5.1.7. Реферат

Не предусмотрено

5.1.8. Проектная работа

Не предусмотрено

5.1.9. Деловая (ролевая) игра / Дебаты / Дискуссия / Круглый стол

Не предусмотрено

5.1.10. Кейс-анализ

Не предусмотрено

5.2. Описание фонда оценочных средств промежуточного контроля по дисциплине модуля

5.2.1. Экзамен /зачет в форме независимого тестового контроля

НТК по дисциплине модуля не проводится.

5.2.2. Зачет в традиционной форме (устные ответы на вопросы экзаменационных билетов)**:**

Перечень примерных вопросов для зачета

1. Типы информационных систем и их характеристика.
2. Цели и основные обязанности администратора информационных систем.

3. Базовые архитектуры, используемые при построении корпоративных информационных сетей.
4. Функциональные области управления, относящиеся к системному администрированию.
5. Компьютерная сеть, характеристики и области применения сетей.
6. Классификации локальных сетей.
7. Активное и пассивное сетевое оборудование.
8. Топология сетей: шина, кольцо, звезда.
9. Кабельные среды для передачи данных по сети.
10. Пакеты и протоколы.
11. Технология хранения данных.
12. Управление дисками и томами.
13. Реализация RAID.
14. Установка Windows Server.
15. Управление службами Windows Server.
16. Управление периферийными и другими устройствами.
17. Обзор технологий виртуализации.
18. Реализация роли Hyper-V.
19. Модель OSI, стек OSI.
20. Модель TCP/IP, обзор основных протоколов.
21. Утилиты диагностики TCP/IP.
22. Адресация в TCP/IP-сетях. Типы адресов стека TCP/IP.
23. Структура IP-адреса. Классы IP-адресов. Особые IP-адреса.
24. Протоколы IPv6 и ARP.
25. Создание таблиц маршрутизации, протоколы маршрутизации RIP и OSPF.
26. Система доменных имен. Служба DNS.
27. Реализация DHCP в Windows. Параметры DHCP.
28. DHCP-сообщения. Принцип работы DHCP.
29. Реализация доменных служб Active Directory.
30. Управление пользователями, группами и компьютерами.
31. Внедрение групповой политики.
32. Обзор модели многоуровневой защиты.
33. Физическая безопасность.
34. Обзор безопасности Windows.
35. Обеспечение безопасности файлов и папок.
36. Обзор сетевой безопасности.
37. Реализация брандмауэров.
38. Защита доступа к сети.
39. Защита электронной почты.
40. Защита серверов.

РАЗДЕЛ 3
ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО МОДУЛЮ
ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 2
БЕЗОПАСНОСТЬ И ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ

Фонд оценочных средств составлен автором(ами):

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Белоусова Вероника Игоревна	к.ф.-м.н	доцент	Департамент информационных технологий и автоматики

Рекомендовано учебно-методическим советом института государственного управления и предпринимательства

Протокол № 10 от 26 июня 2019г.

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ «*БАЗЫ ДАННЫХ*» И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации.

Таблица 1.

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
1	**2**
ПК-8 Способен соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности	**Знать:** – основные принципы работы сети Интернет; – основы HTML; – основы CSS; – основы PHP; – основы использования регулярных выражений; – работу и конфигурирование СУБД MySQL; **Уметь:** – правильно проектировать и реализовывать все основные компоненты – комплексного WEB приложения на практике; – правильно определять и предотвращать основные угрозы для программ в Интернете; **Практический опыт, владение:** – криптографической терминологией; – навыками программной реализации WEB приложения; – навыками использования типовых хэш-функций; – навыками анализа кода на уязвимости; – средствами обеспечения информационной безопасности
ПК-10. Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности	**Знать:** – виды и способы защиты информации при разработке WEB приложений; – криптографические стандарты; – виды и способы разграничения доступа к данным; – перечень основных угроз для программ в сети Интернет. **Уметь:** – находить уязвимые места в коде WEB приложения и устранять их; – использовать регулярные выражения; – настраивать и использовать СУБД MySQL; – уметь реализовывать системы разграниченного доступа на практике; **Практический опыт, владение:** - навыками определения видов и форм информации, подверженных угрозам, и возможных методов и путей устранения этих угроз.

2. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

2.1. Распределение объема времени по видам учебной работы

Таблица 2.

№ п/п	Наименования дисциплины модуля	**Объем времени, отведенный на освоение дисциплины модуля** *3 з.е.*								
		Аудиторные занятия, час.				**Промежуточная аттестация** (форма итогового контроля /час.)	**Контактная работа (час.)**	**Самостоятельная работа студента, включая текущую аттестацию, час.**	**Всего по дисциплине**	
		Занятия лекционного типа	**Практические занятия**	**Лабораторные работы**	**Всего**				**Час.**	**Зач. ед.**
1	*Базы данных*	*17*	*34*	-	*51*	*зачет/4*	*58,9*	*57*	*108*	*3*
Всего на освоение дисциплины модуля (час.)		*17*	*34*	-	*51*	*зачет/4*	*58,9*	*57*	*108*	*3*
								Итого по модулю:	**108**	**3**

2.2.Виды, количество и объем времени на СРС по дисциплине*

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество мероприятий СРС	Объем СРС (час.)
1.	*Подготовка к лекциям*		4 час
2	*Подготовка к практическим занятиям*		*29 час*
3	*Реферат*	*1*	*12 час*
4	*Контрольная работа*	*1*	*8 час*
5	*Подготовка к зачету*	*1*	*4 час*
Итого на СРС по дисциплине:			*57 час.*

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лекций	7 семестр, 1-8	*20*
Контрольная работа	7 семестр, 1-8	*40*
Реферат	7 семестр, 1-8	*40*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,5		
Промежуточная аттестация по лекциям – нет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,5		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение занятий	7 семестр, 9-17	50
Работа на занятиях	7 семестр, 9-17	50
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям–0,5		
Промежуточная аттестация по практическим/семинарским занятиям–зачет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям–0,5**		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Не предусмотрено		
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта–защиты – …		

3.3. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 7	**1**

**В случае проведения промежуточной аттестации по дисциплине (экзамена, зачета) методом тестирования используются официально утвержденные ресурсы: АПИМ УрФУ, СКУД УрФУ, имеющие статус ЭОР УрФУ; ФЭПО (www.фэпо.рф); Интернет-тренажеры (www.i-exam.ru).*

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре критерии (признаки) оценивания достижений студентов на соответствие указанным в табл.1 ФОС индикаторам в рамках контрольно-оценочного мероприятия по дисциплине модуля (табл.4).

Таблица 4

Критерии оценивания результатов обучения

Результаты обучения	**Критерии оценивания результатов обучения на соответствие индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2. Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5.

Шкала оценивания результатов обучения по уровням

Характеристика уровней освоения результатов обучения				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения освоены и в полном объеме соответствуют индикаторам, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)

2.	Результаты обучения освоены и соответствуют индикаторам, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Освоение результатов обучения не в полной мере соответствует индикаторам, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ МОДУЛЯ

Задания по контрольно-оценочным мероприятиям должны обеспечивать освоение результатов обучения и предметного содержания дисциплины и достижение индикаторов на соответствующем уровне.

5.1. Описание оценочных материалов текущего контроля по дисциплине модуля

5.1.1. Практические занятия

Номер занятия	Темы практических занятий	Время на проведение занятия (час.)
1	Основы HTML. Общие положения. Структура HTML-документа. Форматирование текста. Работа с изображениями и мультимедиа. Формы. XHTML. Верстка WEB страниц	8
2	Работа PHP и HTTP. Работа с формами. Передача данных с помощью HTTP запросов. Методы POST и GET. Загрузка файлов на сервер. Работа с Cookies. Работа с HTTP-заголовками. Работа с сессиями. Отличие сессий от Cookies.	6
3	СУБД MySQL. Основы SQL.Типы данных. Операторы. Выражения. Функции PHP для работы с MySQL. Практическое использование MySQL в PHP-приложениях.	4
4	Создание базы данных и таблиц. Получение системных данных. Работа с данными в MySQL.	6

5	Методы обнаружения уязвимостей в web-приложениях.	6
6	Дополнительные механизмы защиты Web-приложений.	4
	Всего:	34

5.1.2. Лабораторные занятия

Не предусмотрено

5.1.3. Курсовая работа / Курсовой проект

Не предусмотрено

5.1.4. Контрольная работа

Примерные варианты заданий контрольных работ:
Примерные задания для домашних работ:

Вариант № 1.
Установка web-сервера и написание простейшей программы «HelloWorld».

Вариант № 2.
Создание HTML страниц на основе представленных изображений.

Вариант № 3.
Расположить блоки с помощью HTML и CSS в заданном порядке.

Вариант № 4.
Сверстать с помощью HTML и CSS страницу из представленного изображения.

Вариант № 5.
Создать фотогалерею с помощью HTML, CSS, PHP. Подгрузку изображений организовать из подпапок, где каждая папка будет являться соответствующим разделом галереи.

Вариант № 6.
Создать страницу с новостями с помощью HTML, CSS, PHP, MySQL. Создать соответствующую базу данных и таблицу с новостями. Вывести новости списком, а также каждую новость подробнее. Новость должна содержать следующие поля:
Дата
Заголовок
Изображение
Краткое содержание
Подробное содержание

Вариант № 7.
Создать страницу с гостевой книгой с помощью HTML, CSS, PHP, MySQL. Создать соответствующую базу данных и таблицу для гостевой книги. Выводить сообщения списком, а также реализовать возможность добавлять собственные сообщения пользователями. Сообщения в гостевой должны содержать следующие поля:
Имя

E-mail
Дата и время
Сообщение

Вариант № 9.
Реализовать регулярные выражения:
Проверить на правильность имя функции
abc //true
i10n //true
10abc //false
abcабвгд //false
abc.3 //false

Вариант № 10.
Реализовать регулярные выражения:
Проверить на число
2010
-1000
10.2
18

Вариант № 11.
Реализовать регулярные выражения:
Проверить на соответствие телефон
+7 (3452) 10-10-10
+7 (343) 100-10-10

Вариант № 12.
Реализовать регулярные выражения:
Проверить IP адресс
192.168.1.1

Вариант № 13.
Реализовать регулярные выражения:
Проверить дату
31-12-1999 //true
31-13-1999 //false

Вариант № 14.
Реализовать регулярные выражения:
Проверить на соответствие любой e-mail
mail@mail.com

Вариант № 15.
Реализовать регулярные выражения:
Получить содержимое тега
<TAG>one<TAG>two</TAG>one</TAG>

Вариант № 16.
Реализовать регулярные выражения:
Проверить пароль на сложность
6 и более символов, цифры, нижнее подчеркивание

Должен содержать хотя бы одну букву в верхнем регистре, одну в нижнем и число

Вариант № 17.
Реализовать регулярные выражения:
Путь до файла в Windows
c://program files/system32/data.dat

Вариант № 18.
Реализовать регулярные выражения:
URL
http://google.com/

Вариант № 19.
Добавить к существующему сайту авторизацию с использованием сессий. Создать соответствующую таблицу с пользователями, где каждый пользователь имеет следующие поля:
Псевдоним
Логин
Пароль, зашифрованный хеш функцией.

Вариант № 20.
Реализовать простейшую систему редактирования содержимого сайта, с возможностью изменять и добавлять новости на сайт только авторизованным пользователям

5.1.5. Домашняя работа

Не предусмотрено

5.1.6. Расчетная работа / Расчетно-графическая работа

Не предусмотрено

5.1.7. Реферат / эссе / творческая работа

Примерный перечень тем рефератов (эссе, творческих работ):

1. Введение в webтехнологии.
2. Основы HTML, использование базовых тегов.
3. Основы CSS, верстка страниц.
4. Комплексное использование HTMLи CSS.
5. Введение в PHP, написание фотогалереи.
6. Введение в MySQL, написание страницы новостей.
7. Введение в MySQL, написание гостевой книги.
8. Регулярные выражения
9. Авторизация и использование сессий.
10. Система редактирования содержимого сайта.
11. Пользовательские функциив PHP.
12. Работа с данными в MySQL
13. Виды уязвимостей

5.1.8. Проектная работа

Не предусмотрено

5.1.9. Деловая (ролевая) игра / Дебаты / Дискуссия / Круглый стол

Не предусмотрено

5.1.10. Кейс-анализ

Не предусмотрено

5.2. Описание фонда оценочных средств промежуточного контроля по дисциплине модуля

5.2.1. Экзамен /зачет в форме независимого тестового контроля

НТК по дисциплине модуля не проводится.

5.2.2. Зачет в традиционной форме (устные /письменные ответы на вопросы экзаменационных билетов)**:**

Примерный перечень вопросов для зачета:

1. Введение в WEB технологии. Основные понятия и определения.
2. Языки программирования для создания интернет приложений. Особенности работы
3. интернет приложений.
4. Основы HTML.Общие сведения. Общие принципы работы языка разметки.
5. Синтаксис.Основы работыс HTML.
6. Основы CSS. Введение в понятие CSS. Принципы работы CSS. Общие положения. Синтаксис.
7. Основы CSS. Псевдоклассы и псевдоэлементы. Свойства CSS. Свойства текста.
8. Свойства шрифта. Свойства цвета и фона. Свойства форматирования и позиционирования.
9. Основы PHP. Общий синтаксис. Переменные и константы. Типы данных.
10. Основы PHP. Операторы. Управляющие конструкции в PHP. Отладка PHP скриптов.
11. Функции в PHP. Пользовательские функциив PHP. Встроенные функции в PHP. Функции для работы с переменными.
12. Функции в PHP.Математические функции. Функции обработки строк. Функции для работы с массивами. Функции даты и времени. Функции для работы с файловой системой.
13. Работа с формами. Передача данных с помощью HTTP запросов. Методы POST и GET. Загрузка файлов на сервер.
14. Работа с Cookies. Работа с HTTP-заголовками. Работа с сессиями. Отличие сессий от Cookies.
15. СУБД MySQL.Основы SQL.Типы данных. Операторы. Выражения. Функции PHP для работы с MySQL.
16. СУБД MySQL.Практическое использование MySQL в PHP-приложениях. Создание базы данных и таблиц.
17. Получение системных данных. Работа с данными в MySQL.
18. Регулярные выражения. Синтаксис регулярных выражений. Основные метасимволы. Символьные классы. Квантификаторы.
19. Регулярные выражения. Модификаторы. Подшаблоны. Позиционные проверки. Функции PHP для работы с регулярными выражениями.
20. Введение в web-безопасность. Статистические данные угроз безопасности ebприложений. Методы обнаружения уязвимостей в web-приложениях.
21. Метод тестирования на проникновение. Генерация запросов по шаблону с типизированными параметрами.
22. Метод статического анализа. Метод динамического анализа.
23. Виды уязвимостей.Уязвимости, приводящие к выполнению кода. Переполнение буфера. Атака на функции форматирования строк. Внедрение операторов LDAP.
24. Выполнение команд операционной системы. Внедрение операторов SQL.

25. Внедрение SQL кода вслепую. Внедрение серверных расширений.
26. Внедрение XML. Внедрение почтовых команд.. Виды уязвимостей, характерные для интернетмагазинов. Дополнительные механизмы защиты Web-приложений.
27. Межсетевые экраны для Web-приложений (WebApplicationFirewalls). Возможности и ограничения WAF. Примеры реализации WAF..

РАЗДЕЛ 3
ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО МОДУЛЮ
АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 3
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Фонд оценочных средств составлен автором(ами):

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Лучинин Александр Сергеевич	к.т.н. доцент	доцент	Департамент радиоэлектроники и связи

Рекомендовано учебно-методическим советом института государственного управления и предпринимательства

Протокол № 10 от 26 июня 2019г.

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ» И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Индикаторы должны учитываться при выборе и составлении заданий контрольно-оценочных мероприятий (оценочных средств) текущей и промежуточной аттестации.

Таблица 1.

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения (индикаторы)**
1	**2**
ПК-8 Способен соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности	**Знать:** – основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; **Уметь:** - выявлять угрозы и технические каналы утечки информации; - описывать (моделировать) объекты защиты и угрозы безопасности информации; **Практический опыт, владение:** – навыками работы с нормативными правовыми актами и контрольно-измерительной аппаратурой; – методами и средствами выявления угроз безопасности информации; – методами технической защиты информации; – методами формирования требований по защите информации; – методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; – профессиональной терминологией.
ПК-10. Способен принимать адекватные и соответствующие законодательству и ситуации управленческие решения в целях обеспечения национальной безопасности	**Знать:** – технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; **Уметь:** - применять наиболее эффективные методы и средства инженерно-технической защиты информации; - контролировать эффективность мер защиты; **Практический опыт, владение:** информации; – методами формирования требований по защите информации; – методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; – профессиональной терминологией.

2. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

2.1. Распределение объема времени по видам учебной работы

Таблица 2.

№ п/п	Наименования дисциплины модуля	Объем времени, отведенный на освоение дисциплины модуля *3 з.е.*								
		Аудиторные занятия, час.				Промежуточная аттестация (форма итогового контроля /час.)	Контактная работа (час.)	Самостоятельная работа студента, включая текущую аттестацию, час.	Всего по дисциплине	
		Занятия лекционного типа	Практические занятия	Лабораторные работы	Всего				Час.	Зач. ед.
1	*Проектирование информационных систем*	*17*	*34*	*-*	*51*	*зачет/4*	*58,9*	*57*	*108*	*3*
Всего на освоение дисциплины модуля (час.)		*17*	*34*	*-*	*51*	*зачет/4*	*58,9*	*57*	*108*	*3*
								Итого по модулю:	**108**	**3**

2.2.Виды, количество и объем времени на СРС по дисциплине*

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество мероприятий СРС	Объем СРС (час.)
1.	*Подготовка к лекциям*		*3 час*
2	*Подготовка к практическим занятиям*		*26 час*
3	*Домашняя работа*	*1*	*12 час*
4	*Реферат*	*1*	*12 час*
5	*Подготовка к зачету*	*1*	*4 час*
		Итого на СРС по дисциплине:	*57 час.*

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5

Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лекций	7 семестр, 1-8	*20*
Домашняя работа	7 семестр, 1-8	*40*
Контрольная работа	7 семестр, 1-8	*40*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,5		
Промежуточная аттестация по лекциям – нет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,5		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение занятий	7 семестр, 9-17	50
Работа на занятиях	7 семестр, 9-17	50
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям–0,5		
Промежуточная аттестация по практическим/семинарским занятиям–зачет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям–0,5**		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Не предусмотрено		
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта–защиты – …		

3.3. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 7	**1**

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре критерии (признаки) оценивания достижений студентов на соответствие указанным в табл.1 ФОС индикаторам в рамках контрольно-оценочного мероприятия по дисциплине модуля (табл.4).

Таблица 4

Критерии оценивания результатов обучения

Результаты обучения	**Критерии оценивания результатов обучения на соответствие индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2. Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5.

Шкала оценивания результатов обучения по уровням

Характеристика уровней освоения результатов обучения				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения освоены и в полном объеме соответствуют индикаторам, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения освоены и соответствуют индикаторам, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)

3.	Освоение результатов обучения не в полной мере соответствует индикаторам, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ МОДУЛЯ

Задания по контрольно-оценочным мероприятиям должны обеспечивать освоение результатов обучения и предметного содержания дисциплины и достижение индикаторов на соответствующем уровне.

5.1. Описание оценочных материалов текущего контроля по дисциплине модуля

5.1.1. Практические занятия

Номер занятия	Темы практических занятий	Время на проведение занятия (час.)
1	Классификация способов и средств защиты объектов информатизации.	4
2	Классификация способов и средств защиты помещений от утечки речевой информации по техническим каналам.	4
3	Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	4
4	Показатели эффективности защиты речевой информации.	4
5	Методы выявления электронных устройств негласного получения информации, внедренных в помещения и технические средства.	4
6	Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации.	4
7	Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты.	4
8	Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации.	4

9	Порядок документального оформления результатов аттестационных испытаний и соответствия объекта информатизации требованиям по безопасности информации	2
	Всего:	34

5.1.2. Лабораторные занятия

Не предусмотрено

5.1.3. Курсовая работа / Курсовой проект

Не предусмотрено

5.1.4. Контрольная работа

Примерная тематика контрольных работ:

1. Методы и технические средства съема конфиденциальной речевой информации с использованием вторичных переизлучателей.
2. Методы и технические средства съема конфиденциальной речевой информации с использованием опто-волоконных линий связи.
3. Методы и технические средства съема конфиденциальной речевой информации с использованием средств высокочастотного навязывания.
4. Технические средства подслушивания, методы и средства противодействия средствам подслушивания.
5. Технические средства контроля, обнаружения, уничтожение закладных устройств, порядок проведения ЗПМ.
6. Технические средства контроля, обнаружения, уничтожение закладных устройств, в слаботочных линиях связи, порядок проведения ЗПМ.
7. Технические средства контроля, обнаружения, уничтожение закладных устройств в телефонных линиях связи, порядок проведения ЗПМ.
8. Технические средства контроля, обнаружения, уничтожение закладных устройств, в электросетях, цепях заземления, порядок проведения ЗПМ.
9. Способы и средства контроля и порядок проведения ЗПМ в защищаемых помещений на отсутствие закладных устройств.
10. Моделирование вербального объекта защиты, возможных угроз безопасности информации для оптических каналов утечки информации в видимом и ИК диапазонах, разработка способов, методов и технических средств защиты информации.
11. Математические методы моделирования для вербального объекта защиты от возможных угроз безопасности информации для акустических каналов утечки информации.
12. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустических каналов утечки информации, разработка методов и технические средств защиты информации.
13. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для кустикорадиэлектронных каналов утечки информации, разработка методов и технических средств защиты информации.
14. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустико-оптических каналов утечки информации, разработка методов и технических средств защиты информации.
15. Моделирование вербального объекта защиты, где производится обработка информации с использованием СВТ (АС), возможных угроз безопасности информации и

технических каналов утечки информации, разработка методов и технических средств защиты информации.

16. Моделирование вербального объекта защиты, где производится обработка информации с использованием технических средств обработки информации, возможных угроз безопасности информации и технических каналов утечки информации, разработка методов и технических средств защиты информации.

Моделирование вербального объекта защиты, возможных угроз безопасности информации для материально-вещественных каналов утечки информации, разработка методов и технических средств защиты информации.

5.1.5. Домашняя работа

Примерная тематика домашних работ:

17. Демаскирующие признаки объектов информатизации;
18. Принципы работы и характеристики технических средств несанкционированного съема акустической информации;
19. Принципы миниатюризации и камуфлирования средств разведки под бытовые приборы. Деконспирационные признаки;
20. Порядок организации защиты информации от утечки по техническим каналам на объектах информатизации и в помещениях на различных этапах жизненного цикла объекта защиты.
21. Программно-аппаратные комплексы для проведения специальных исследований СВТ на ПЭМИН;
22. Программно-аппаратные комплексы для проведения акустических и виброакустических измерений;
23. Методы закрытия прямых акустических, вибрационных и оптико-электронных каналов перехвата речевой информации. Анализ уязвимости каналов и определение способов их закрытия;
24. Программно-аппаратные комплексы для поиска и обнаружения демаскирующих признаков закладных устройств различного рода
25. Характеристики речевого сигнала. Разборчивость речи.
26. Комплексный подход к построению технической защиты информации на объекте
27. информатизации.
28. Основные положения и принципы построения технической защиты информации.
29. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты.
30. Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.
31. Модель поведения инсайдера на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам.
32. Условия и факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.
33. Условия и субъективные факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации.
34. Методы защиты видовых демаскирующих признаков от технических средств.
35. Методы защиты сигнальных демаскирующих признаков от технических средств.
36. Методы защиты радиосигналов от перехвата техническими средствами.
37. Методы защиты электрических сигналов от перехвата техническими средствами.
38. Методы защиты материальных и вещественных демаскирующих признаков от
39. технических средств.
40. Технические средства наблюдения в видимом и ИК диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.

41. Технические средства наблюдения в радио диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.
42. Технические средства перехвата конфиденциальной информации передаваемой по линии связи, методы и средства противодействия перехвата конфиденциальной информации.
43. Порядок проведения аттестационных испытаний по требованиям безопасности информации на примере вербального объекта информатизации. Порядок проведения работ по созданию системы защиты информации для вербального объекта информатизации.
44. Организационные методы контроля эффективности защиты информации на примере вербального объекта информатизации.
45. Технические средства контроля эффективности защиты информации на примере вербального объекта информатизации.

5.1.6. Расчетная работа / Расчетно-графическая работа.

Не предусмотрено

5.1.7. Реферат / эссе / творческая работа

Не предусмотрено

5.1.8. Проектная работа

Не предусмотрено

5.1.9. Деловая (ролевая) игра / Дебаты / Дискуссия / Круглый стол

Не предусмотрено

5.1.10. Кейс-анализ

Не предусмотрено

5.2. Описание фонда оценочных средств промежуточного контроля по дисциплине модуля

5.2.1. Экзамен /зачет в форме независимого тестового контроля

НТК по дисциплине модуля не проводится.

5.2.2. Зачет в традиционной форме (устные /письменные ответы на вопросы экзаменационных билетов)**:**

Примерный перечень вопросов:

1. Объект информатизации (определение).
2. Основные технические средства и системы (ОТСС).
3. Вспомогательные технические средства и системы (ВТСС).
4. Технический канал утечки информации (определение). Схема технического канала утечки информации
5. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).
6. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений.
7. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений.
8. Линейные и энергетические характеристики акустического поля. Основные характеристики речи и речевого сигнала. Разборчивость речи.

9. Классификация технических каналов утечки акустической (речевой) информации и способов перехвата речевой информации.
10. Средства акустической разведки: цифровые диктофоны, направленные микрофоны (классификация, характеристики, основные возможности, схема канала перехвата).
11. Дальность перехвата речевого сигнала средством акустической разведки направленными микрофонами.
12. Схемы перехвата речевой информации по акустовибрационному каналу утечки речевой информации. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.
13. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.
14. Экранирующие материалы, их основные характеристики. Формула для расчета коэффициента экранирования для электрической и магнитной составляющей электромагнитного поля.
15. Экранированные помещения и экранированные камеры (классификация, состав, основные характеристики).
16. Основные требования к заземлению технических средств. Схемы заземлителей.
17. Схемы заземления технических средств. Схемы измерения сопротивления заземления технических средств.
18. Основные требования к системе пространственного электромагнитного зашумления.
19. Схема установки системы пространственного зашумления на объекте информатизации.
20. Основные требования по установке системы пространственного зашумления на объекте информатизации.
21. Основные характеристики генераторов шума.
22. Основные требования к системе электропитания технических средств.
23. Способы защиты цепей электропитания технических средств от утечки информации, возникающей за счет наводок побочных электромагнитных излучений.
24. Основные требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания технических средств.
25. Основные характеристики фильтров нижних частот (ФНЧ).
26. Схемы установки помехоподавляющих фильтров на объекте информатизации.
27. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.
28. Средства звуко- и виброизоляции выделенных помещений. Звукоизолирующие кабины. Специальные защищенные помещения.
29. Порядок проведения контроля эффективности защиты ВТСС.
30. Состав и основные требования к аппаратуре контроля при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.
31. Схема измерительной установки при контроле ВТСС на подверженность акустоэлектрическим преобразованиям.
32. Порядок проведения проверки ВТСС на подверженность акустоэлектрическим преобразованиям.
33. Состав и основные требования к аппаратуре контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.
34. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.
35. Сканирующие приемники (принцип работы, основные характеристики). Этапы выявления РЗ.
36. Методы обнаружения, идентификации РЗ и определения их местоположения.
37. Порядок организации защиты информации на объектах информатизации.
38. Предварительное специальное обследование объекта информатизации.

39. Аналитическое обоснование необходимости создания СТЗИ объекта (содержание, порядок проведения).
40. Замысел создания СТЗИ. Техническое задание на разработку СТЗИ объекта информатизации.
41. Организация аттестации объекта информатизации по требованиям безопасности информации. Перечень документов, предоставляемых Заявителем для проведения аттестации объекта информатизации.
42. Порядок проведения аттестации объекта информатизации по требованиям безопасности информации. 26. Заключение по результатам аттеста