МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Удалённый и непосредственный несанкционированный доступ в распределённых компьютерных системах»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация Безопасность распределенных компьютерных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /А.Е. Дешина/

Заведующий кафедрой Систем информационной безопасности _____ / А.Г. Остапенко /

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины

Изучение методологии анализа информационных рисков и управления защищенностью РКС от воздействий угроз непосредственного и удаленного доступа к ее элементам.

1.2.Задачиосвоениядисциплины

-Освоение процессов представления, анализа и обоснования моделей, методов и механизмов обеспечения компьютерной безопасности;

-Обучение методологии анализа архитектурных (схемно-технических) и программно-алгоритмических решений, применяемых в системах защиты информации современных компьютерных систем.

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Удалённыйинепосредственныйнесанкционированныйдоступвраспределённыхкомпьютерныхсистемах»относитсякдисциплинамвариативнойчастиблокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Удалённыйинепосредственныйнесанкционированныйдоступвраспределённыхкомпьютерныхсистемах»направленнаформированиеследующихкомпетенций:

ПК-12-способностьюпроводитьинструментальныймониторингзащищенностикомпьютерныхсистем

ПК-14-способностьюорганизовыватьработыповыполнениюрежимазащитыинформации,втомчислеограниченногодоступа

ПСК-3.2 - способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ПК-12	Знать защитные механизмы и средства обеспечения сетевой безопасности
	Уметьразрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	Владетьнавыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений
ПК-14	Знать принципы и особенности функционирования

	проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов; принципы функционирования, технические и конструктивные решения ориентированные на методы и технологии хранения данных, в том числе на базе современных серверных операционных систем;
	Уметь разрабатывать и применять современные проблемно-ориентированные системы управления, принятия решения и оптимизации технических объектов;
	Владеть навыками работы с программно-аппаратными средствами хранения, управления и конфигурирования данных; навыками решения задач обработки данных на основе современных методов, моделей и инструментальных средств, реализующих функции анализа, управления добычи и визуализации данных.
ПСК- 3.2	Знать структуру систем защиты информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем
	Уметь пользоваться нормативными документами по противодействию технической разведке
	Владеть методами расчета и инструментального контроля показателей технической защиты информации

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Удалённыйинепосредственныйнесанкционированныйдоступвраспределённыхкомпьютерныхсистемах»составляет 7з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всего часов	Семестры	
		9	10
Аудиторныезанятия (всего)	72	36	36
В томчисле:			
Лекции	36	18	18
Лабораторныеработы (ЛР)	36	18	18
Самостоятельнаяработа	144	72	72
Курсовойпроект	+	+	
Часынаконтроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 252 7	 108 3	 144 4

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

		9-ый семестр				
№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. зан.	СРС	Всего, час
1	РКС как объект атак, связанных с удаленным и непосредственным доступом к ее элементам	РКС как объект атак, связанных с удаленным и непосредственным доступом к ее элементам.Содержание и структура понятия РКС.Общая характеристика принципов, методов и механизмов проведения атак на РКС, связанных с удаленным и непосредственным доступом к ее элементам.Угрозы безопасности в РКС .Понятие угроз безопасности и их классификация и идентификация. Методы	4	4	24	32

		оценивания угроз. Политика и модели безопасности РКС. Понятие политики и моделей безопасности информации в РКС. Субъектно-объектная модель РКС в механизмах и процессах коллективного доступа к информационным ресурсам. Монитор безопасности и основные типы политик безопасности. Гарантирование выполнения политики безопасности.				
2	Меры и средства защиты от атак, связанных с непосредственным и удаленным доступом к элементам РКС	Модели безопасности РКС на основе дискреционной политики. Общая характеристика моделей дискреционного доступа. Пятимерное пространство Хартсона. Модели на основе матрицы доступа. Модели распространения прав доступа. Общая характеристика политики мандатного доступа. Модель Белла-ЛаПадулы и ее расширения.Основные расширения модели Белла-ЛаПадулы.Общая характеристика тематического разграничения доступа. Тематические решетки. Модель тематико-иерархического разграничения доступа. Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений. Формальная спецификация и	4	4	24	32

		разновидности ролевых моделей. Индивидуально-групповое разграничение доступа.				
3	Приложения сетевой защиты	Приложения аутентификации. Система Kerberos. Отказоустойчивость и виртуализация локальных сетей. Протокол STP ,RSTP. Фильтрация трафика. Адресация и технология CIDR. Протокол Proxy-ARP.Система DNS	10	10	24	44
		Итого за 9-ый семестр	**18**	**18**	**72**	**108**
10-ый семестр						
№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. зан.	СРС	Всего, час
4	Аналитическое моделирование процессов реализации угроз непосредственного и удаленного доступа к элементам РКС.	Понятие и общая характеристика скрытых каналов утечки информации в РКС. Модели информационного невмешательства и информационной невыводимости. Нейтрализация скрытых каналов утечки информации на основе технологий «представлений» и «разрешенных процедур». Общая характеристика моделей и технологий обеспечения целостности данных в РКС. Дискреционная модель Кларка-Вильсона. Мандатная модель Кена Биба. Технологии параллельного выполнения транзакций в клиент-серверных системах (СУБД).	4	4	24	32
5	Меры и средства защиты от атак, связанных с непосредственным доступом к элементам РКС	Меры контроля физического доступа к элементам РКС. Технологии аутентификации.	4	4	24	32

		Аутентификация на основе паролей. Аутентификация на основе аппаратных аутентификаторов. Электронная подпись. Формы представления ограничений доступом. Протокол SSH. Централизованные системы аутентификации и авторизации				
6	Уязвимости ИТКС в отношении угроз удаленного доступа	Классификация удаленных атак. Технологии безопасности на основе фильтрации и мониторинга трафика. Виды фильтрации. Прокси-серверы. Файерволы с функцией NAT. Трансляция сетевых адресов и портов. Система мониторинга NetFloy	10	10	24	44
Итого за 10-ый семестр			**18**	**18**	**72**	**108**
Итого			**36**	**36**	**144**	**216**

5.2Переченьлабораторныхработ

Неделя семестра	Тема и содержание практического занятия	Объемчасов	В том числе, в интерактивной форме (ИФ)	Видыконтроля
1	2	3	4	
9 семестр		**18**		Зачет с оценкой
1 РКС как объект атак, связанных с удаленным и непосредственным доступом к ее элементам		**8**		
1	Изучение современных принципов, методов и механизмов обеспечения компьютерной безопасности в РКС.	2		

2	Оценивание угроз безопасности в распределенных компьютерных системах.	2		
3	Реализация политик учётных записей в современных операционных системах.	2		
4	Реализация политик аудита в современных РКС.	2		
2 Меры и средства защиты от атак, связанных с непосредственным и удаленным доступом к элементам РКС		**8**		
6	Исследование сценариев атак на распределенные компьютерные системы, функционирующие на основе модели HRU.	2		
7	Исследование сценариев атак на распределенные компьютерные системы, функционирующие на основе модели TAM.	2		
9	Исследование сценариев атак на распределенные компьютерные системы, функционирующие на основе расширенной модели TAKE-GRANT.	2		
10	Оптимизация прав доступа в распределенных компьютерных системах, функционирующих на основе модели Белла-ЛаПадуллы.	2		
10 семестр		**18**		Экзамен
3 Аналитическое моделирование процессов реализации угроз непосредственного и удаленного доступа к элементам РКС.		**10**		
1-2	Изучение положений ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общиеположения».	2		
3-4	Изучение положений ГОСТ Р 53113.2-2009 «Информационная технология. Защита	2		

	информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов».			
5	Практическая реализация дискреционной модели Кларка-Вильсона обеспечения целостности данных в РКС.	2		
6	Практическая реализация мандатной модели Биба обеспечения целостности данных в РКС.	2		
7	Способы и средства резервирования, архивирования и журнализация в современных операционных системах.	2		
4 МЕТОДЫ АНАЛИЗА И ОЦЕНКИ ЗАЩИЩЕННОСТИ РКС		**8**		
10	Моделирование процессов реализации угроз удаленного доступа к распределенным компьютерным системам.	2		
12	Программные средства удаленного доступа к РКС.	2		
13-14	Меры и средства защиты от атак, связанных с удаленным доступом к РКС.	2		
17	Изучение положений Руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.», «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.»	2		
Итогочасов		**36**		

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплиныпредусматриваетвыполнениекурсовогопроектав9семестредляочнойформыобучения.

Примернаятематикакурсовогопроекта:«Моделирование атак на транспортную инфраструктуру РКС»(по вариантам)

Курсовойпроектвключатвсебяграфическуючастьирасчетно-пояснительнуюзаписку.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениванияикомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-12	Знать защитные механизмы и средства обеспечения сетевой безопасности	Знание защитных механизмов и средств обеспечения сетевой безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Умение разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных	Владение навыками анализа основных характеристик и возможностей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	сообщений	телекоммуникационных систем по передаче оперативных и специальных сообщений		
ПК-14	Знать принципы и особенности функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов;	Знание принципов и особенностей функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь разрабатывать и применять современные проблемно-ориентированные системы управления, принятия решения и оптимизации технических объектов;	Умение разрабатывать и применять современные проблемно-ориентированные системы управления, принятия решения и оптимизации технических объектов;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками работы с программно-аппаратными средствами хранения, управления и конфигурирования данных; навыками решения задач обработки данных на основе современных методов, моделей и инструментальных средств, реализующих функции анализа, управления добычи и визуализации данных.	Владение навыками работы с программно-аппаратными средствами хранения, управления и конфигурирования данных; навыками решения задач обработки данных на основе современных методов, моделей и инструментальных средств, реализующих функции анализа, управления добычи и визуализации данных.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК- 3.2	Знать структуру систем защиты информации в распределенных	Знание структурысистем защиты	Выполнение работ в срок, предусмотренный в	Невыполнение работ в срок, предусмотренн

	компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем	информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки защищенности распределенных компьютерных систем Умение пользоваться нормативными документами по противодействию технической разведке Владение методами расчета и инструментального контроля показателей технической защиты информации	рабочих программах	ый в рабочих программах
	Уметь пользоваться нормативными документами по противодействию технической разведке			
	Владеть методами расчета и инструментального контроля показателей технической защиты информации			

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв9,10семестре дляочнойформыобученияподвух/четырехбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
ПК-12	Знать защитные механизмы и средства обеспечения сетевой безопасности	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Решениестандартныхпрактическихзадач	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

	Владеть навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
ПК-14	Знать принципы и особенности функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов;	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь разрабатывать и применять современные проблемно-ориентированные системы управления, принятия решения и оптимизации технических объектов;	Решениестандартныхпрактическихзадач	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
	Владеть навыками работы с программно-аппаратными средствами хранения, управления и конфигурирования данных; навыками решения задач обработки данных на основе современных методов, моделей и инструментальных средств, реализующих функции анализа, управления добычи и визуализации данных.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
ПСК- 3.2	Знать структуру систем защиты информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%

	распределенных компьютерных систем			
	Уметь пользоваться нормативными документами по противодействию технической разведке	Решениестандартныхпрактическихзадач	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
	Владеть методами расчета и инструментального контроля показателей технической защиты информации	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилииныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1) Что такое политики безопасности?
   a. Пошаговые инструкции по выполнению задач безопасности
   b. Общие руководящие требования по достижению определенного уровня безопасности
   c. Широкие, высокоуровневые заявления руководства
   d. Детализированные документы по обработке инцидентов безопасности

2) Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
   a. гаммирования;
   b. подстановки;
   c. кодирования;
   d. перестановки;

3) Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
   a. гаммирования;
   b. подстановки;
   c. кодирования;
   d. перестановки;

4) Защита информации это:

a. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
b. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
c. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
d. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

5) Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:
   a. детектор;
   b. доктор;
   c. сторож;
   d. ревизор;

6) На каком уровне эталонной модели OSI**чаще** всего **не** функционирует комплексный экран?
   a. Прикладной
   b. Сеансовый
   c. Транспортный
   d. сетевой

7) Компьютерные вирусы – это:
   a. программы,способные к саморазмножению(самокопированию);
   b. файлы,имеющие определенное расширение;
   c. файлы,которые невозможно удалить;
   d. программы,сохраняющиеся в оперативной памяти после выключения компьютера;

8) Какие программы не относятся к антивирусным?
   a. программы-ревизоры;
   b. программы-мониторы;
   c. программы-фаги;
   d. программы сканирования;

9) Какой метод обнаружения использует маски вирусов?
   a. метод сравнения с эталоном;
   b. эвристический анализ;
   c. антивирусный мониторинг;
   d. метод обнаружения изменений;

10) К какой среде обитания относятся документы word?
   a. Файловые;
   b. Загрузочные;
   c. Макро;
   d. Сетевые.

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

11) Для безопасной передачи данных по каналам открытых глобальных сетей, в частности Интернет, используется технология:
   a. DICOM
   b. VPN
   c. FTP
   d. XML

12) Какой протокол не относится к протоколам аутентификации удаленных пользователей?
   a. FTP
   b. PAP
   c. CHAP
   d. S/Key

13) В каком протоколе пароль каждого пользователя для передачи по линии связи шифруется на основе случайного числа полученного от сервера?
   a. FTP
   b. PAP
   c. CHAP
   d. S/Key

14) Какому уровню модели OSI протоколIPSec обеспечивает защиту?
   a. Сетевой
   b. Транспортный
   c. Сеансовый
   d. Представительский

15) Какой протокол обеспечивает безопасную передачу данных по сетям IP?
   a. SOCKS
   b. FTP
   c. IPSec
   d. PPTP

16) Какой протокол не участвует в функционировании прикладного шлюза МЭ?
   a. HTTP
   b. FTP

c. Telnet
d. IPSec

17) Какая техническая реализацияVPN осуществляет шифрование специализированными микросхемами?
a. На основе маршрутизаторов
b. На основе межсетевых экранов
c. На основе программных решений
d. На основе специализированных аппаратных средств

18) Какой протокол позволяет передавать по сети одноразовый пароль в открытом виде?
a. S/Key
b. PAP
c. CHAP
d. PPTP

19) Какой протокол позволяет согласовывать алгоритмы и математические структуры (так называемые мультипликативные группы, определенные на конечном поле) для процедуры обмена ключами Диффи — Хеллмана, а также процессов аутентификации?
a. Oakley
b. ISAKMP
c. L2TP
d. L2F

20) Каким протоколом обеспечивается эффективность использования для выполнения функций посредничества его ориентацией на сеансовый уровень модели OSI?
a. HTTP
b. FTP
c. SOCKS
d. SMTP

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

(минимум10вопросовдлятестированиясвариантамиответов)

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

1. РКС как объект атак, связанных с удаленным и непосредственным доступом к ее элементам.

2. Содержание и структура понятия РКС.

3.Общая характеристика принципов, методов и механизмов проведения атак на РКС, связанных с удаленным и непосредственным доступом к ее элементам.

4. Угрозы безопасности в РКС .

5. Понятие угроз безопасности и их классификация и идентификация. Методы оценивания угроз.

6. Политика и модели безопасности РКС. Понятие политики и моделей

безопасности информации в РКС.

7. Субъектно-объектная модель РКС в механизмах и процессах коллективного доступа к информационным ресурсам.

8. Монитор безопасности и основные типы политик безопасности. Гарантирование выполнения политики безопасности. Модели безопасности РКС на основе дискреционной политики. Общая характеристика моделей дискреционного доступа.

9. Пятимерное пространство Хартсона.

10. Модели на основе матрицы доступа. Модели распространения прав доступа.

11. Общая характеристика политики мандатного доступа.

12. Модель Белла-ЛаПадулы и ее расширения. Основные расширения модели Белла-ЛаПадулы.

13. Общая характеристика тематического разграничения доступа. Тематические решетки. 14. Модель тематико-иерархического разграничения доступа.

15. Общая характеристика моделей разграничения доступа на основе функционально-ролевых отношений. Формальная спецификация и разновидности ролевых моделей.

16. Индивидуально-групповое разграничение доступа. Приложения аутентификации.

17. Система Kerberos.

18. Отказоустойчивость и виртуализация локальных сетей.

19. Протокол STP , RSTP.

20. Фильтрация трафика.

21. Адресация и технология CIDR.

22. Протокол Proxy-ARP.

23. Система DNS

7.2.5Примерныйпереченьвопросовдляэкзамена

1.Понятие и общая характеристика скрытых каналов утечки информации в РКС.

2. Модели информационного невмешательства и информационной невыводимости.

3. Нейтрализация скрытых каналов утечки информации на основе технологий «представлений» и «разрешенных процедур».

4.Общая характеристика моделей и технологий обеспечения целостности данных в РКС. Дискреционная модель Кларка-Вильсона.

5.Мандатная модель Кена Биба.

6.Технологии параллельного выполнения транзакций в клиент-серверных системах (СУБД).

7. Меры контроля физического доступа к элементам РКС.

8. Технологии аутентификации.

9. Аутентификация на основе паролей.

10. Аутентификация на основе аппаратных аутентификаторов.

11. Электронная подпись.

12. Формы представления ограничений доступом.

13. Протокол SSH.

14. Централизованные системы аутентификации и авторизации. Классификация удаленных атак.

15.Технологии безопасности на основе фильтрации и мониторинга трафика.

16. Виды фильтрации.

17. Прокси-серверы.

18. Файерволы с функцией NAT.

19. Трансляция сетевых адресов и портов.

20. Система мониторинга NetFloy

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

(Зачетиэкзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	РКС как объект атак, связанных с удаленным и непосредственным доступом к ее элементам	ПК-12, ПК-14, ПСК-3.2	Тест, контрольная работа, защита лабораторных работ, защита реферата
2	Меры и средства защиты от атак, связанных с непосредственным и удаленным доступом к элементам РКС	ПК-12, ПК-14, ПСК-3.2	Тест, контрольная работа, защита лабораторных работ, защита реферата
3	Приложения сетевой защиты	ПК-12, ПК-14, ПСК-3.2	Тест, контрольная работа, защита лабораторных работ, защита реферата
4	Аналитическое моделирование процессов реализации угроз непосредственного и удаленного доступа к элементам РКС	ПК-12, ПК-14, ПСК-3.2	Тест, контрольная работа, защита лабораторных работ, защита реферата,
5	Меры и средства защиты от атак, связанных с непосредственным доступом к элементам РКС	ПК-12, ПК-14, ПСК-3.2	Тест, контрольная работа, защита лабораторных работ, защита реферата,
6	Уязвимости ИТКС в отношении угроз удаленного доступа	ПК-12, ПК-14, ПСК-3.2	Тест, контрольная работа, защита лабораторных работ, защита реферата,

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении

промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампрактикосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымвметодическихматериалах.Примерноевремязащитынаодногостудентасоставляет20мин.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

1. Радько Н.М. Риск-модели информационно - телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н. М. Радько, И. О. Скобелев; под ред. В. И. Борисова. - М.: РадиоСофт, 2010. - 232 с. - ISBN 978-5-93274-019-4: 300-00.
2. Белоножкин В.И. Автоматизированные защищенные системы [Электронный ресурс]: Учеб. пособие / В. И. Белоножкин. - Электрон. текстовые, граф. дан. (1.38 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.
3. Кащенко Г.А. Защита программного обеспечения от несанкционированного использования [Электронный ресурс]: Учеб. пособие / Г. А. Кащенко. - Электрон. текстовые, граф. дан. (559 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

Дополнительная литература:

1. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа [Электронный ресурс]: Учеб. пособие / Н. М. Радько, Ю. К. Язов. - Электрон. текстовые, граф. дан. (1,62 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.
2. Радько, Н.М. Проникновения в операционную среду компьютера: модели злоумышленного непосредственного доступа [Электронный

ресурс]: Учеб. пособие / Н. М. Радько, Ю. К. Язов. - Электрон. текстовые, граф. дан. (1,27 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

3. Остапенко А.Г. Обнаружение и нейтрализация вторжений в распределенных информационных системах [Электронный ресурс]: Учеб. пособие / А. Г. Остапенко, М. Н. Иванкин. - Электрон. текстовые, граф. дан. (366 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

8.2Переченьинформационныхтехнологий,используемыхприосуществлениинобразовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
https://marsohod.org/howtostart/marsohod2
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Удалённыйинепосредственныйнесанкционированныйдоступвраспределённыхкомпьютерныхсистемах»читаютсялекции,проводятсялабораторныеработы,выполняетсякурсовойпроект.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Методикавыполнениякурсовогопроектаизложенавучебно-методическомпособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременноивустанов

ленныесроки.

Контрольусвоенияматериаладисциплиныпроизводитсяпроверкойкурсовогопроекта,защитойкурсовогопроекта.

Видучебныхзанятий	Деятельностьстудента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторнаяработа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельнаяработа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточнойаттестации.
Подготовка к промежуточнойаттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.