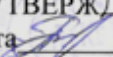


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

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

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

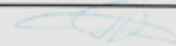
Автор программы

 /А.Е. Дешина/

Заведующий кафедрой
Систем информационной
безопасности

 / А.Г. Остапенко /

Руководитель ОПОП

 / А.Г. Остапенко /

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

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

1.2. Задачи освоения дисциплины

- 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. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Удалённый и непосредственный несанкционированный доступ в распределённых компьютерных системах» относится к дисциплинам вариативной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Удалённый и непосредственный несанкционированный доступ в распределённых компьютерных системах» направлен на формирование следующих компетенций:

ПК-12-способностью проводить инструментальный мониторинг защищенности компьютерных систем

ПК-14-способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа

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

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-12	Знать защитные механизмы и средства обеспечения сетевой безопасности
	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	Владеть навыками 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

Общая трудоемкость дисциплины «Удалённый и непосредственный несанкционированный доступ в распределённых компьютерных системах» составляет 10 з.е.

Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	126	36	90
В том числе:			
Лекции	72	18	54
Практические занятия (ПЗ)	54	18	36
Самостоятельная работа	198	72	126
Курсовой проект	+	+	
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость:			
академические часы	360	108	252
зач.ед.	10	3	7

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий очная форма обучения

№ п/п	Наименование темы	9-ый семестр	Лекц	Практ. раб.	СРС	Всего, час
		Содержание раздела				
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 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.	4	4	24	32
2	Меры и средства защиты от атак, связанных с удаленным и непосредственным 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	4	4	24	32

		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 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	Наименование темы	Содержание раздела	Лекц	Практ. раб.	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	14	12	42	68

		системах (СУБД).				
5	Меры и средства защиты от атак, связанных с непосредственным доступом к элементам РКС	Меры контроля физического доступа к элементам РКС. Технологии аутентификации. Аутентификация на основе паролей. Аутентификация на основе аппаратных аутентификаторов. Электронная подпись. Формы представления ограничений доступом. Протокол SSH. Централизованные системы аутентификации и авторизации	20	12	42	74
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	20	12	42	74
Итого за 10-ый семестр			54	36	126	216
Итого			72	54	198	324

5.2 Перечень лабораторных работ

Непредусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 9 семестре для очной формы обучения.

Примерная тематика курсового проекта: «Моделирование атак на транспортную инфраструктуру РКС» (по вариантам)

Курсовой проект включает в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-12	Знать защитные механизмы и средства обеспечения сетевой безопасности	Знание защитных механизмов и средств обеспечения	Выполнение работ в срок, предусмотренный	Невыполнение работ в срок, предусмотренный

		сетевой безопасности	в рабочих программах	й 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 потокам	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренны й в рабочих программах
	Владеть навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче оперативных и специальных сообщений	Владение навыками анализа основных характеристик и возможностей телекоммуникационн ых систем по передаче оперативных и специальных сообщени	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренны й в рабочих программах
ПК-14	Знать принципы и особенности функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов;	Знание принципов и особенностей функционирования проблемно-ориентир ованных систем управления, принятия решений и оптимизации технических объектов;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренны й в рабочих программах
	Уметь разрабатывать и применять современные проблемно-ориентированные системы управления, принятия решения и оптимизации технических объектов;	Умение разрабатывать и применять современные проблемно-ориентир ованные системы управления, принятия решения и оптимизации технических объектов;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренны й 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	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренны й в рабочих программах

		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	Знание структуры систем защиты информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки защищенности распределенных компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь пользоваться нормативными документами по противодействию технической разведке	Умение пользоваться нормативными документами по противодействию технической разведке		
	Владеть методами расчета и инструментального контроля показателей технической защиты информации	Владение методами расчета и инструментального контроля показателей технической защиты информации		

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9, 10 семестре для очной формы обучения по двух/четырёхбалльной системе:

«зачтено»

«незачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Незачтено
ПК-12	Знать защитные механизмы и средства обеспечения сетевой безопасности	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть навыками анализа основных характеристик и возможностей телекоммуникационных	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	систем по передаче оперативных и специальных сообщений			
ПК-14	Знать принципы и особенности функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов;	Тест	Выполнение теста на 70-100%	Выполнение не менее 70%
	Уметь разрабатывать и применять современные проблемно-ориентированные системы управления, принятия решения и оптимизации технических объектов;	Решение стандартных практических задач	Продемонстрировать верный ход решения в большинстве задач	Задачи решены
	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	Продемонстрировать верный ход решения в большинстве задач	Задачи решены
ПСК- 3.2	Знать структуру систем защиты информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем	Тест	Выполнение теста на 70-100%	Выполнение не менее 70%
	Уметь пользоваться нормативными документами по противодействию технической разведке	Решение стандартных практических задач	Продемонстрировать верный ход решения в большинстве задач	Задачи решены

	Владеть методами расчета и инструментального контроля показателей технической защиты информации	Решение прикладных задач в конкретной предметной области	Продемонстрировать верный ход решения в большинстве задач	Задачи решены
--	---	--	---	---------------

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

- 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.

7.2.2 Примерный перечень заданий для решения стандартных задач

- 11) Для безопасной передачи данных по каналам открытых глобальных сетей, в частности Интернет, используется технология:
- DICOM
 - VPN
 - FTP
 - XML
- 12) Какой протокол не относится к протоколам аутентификации удаленных пользователей?
- FTP
 - PAP
 - CHAP
 - S/Key
- 13) В каком протоколе пароль каждого пользователя для передачи по линии связи шифруется на основе случайного числа полученного от сервера?
- FTP
 - PAP
 - CHAP
 - S/Key
- 14) Какому уровню модели OSI протокол IPSec обеспечивает защиту?
- Сетевой
 - Транспортный
 - Сеансовый
 - Представительский
- 15) Какой протокол обеспечивает безопасную передачу данных по сетям IP?
- SOCKS
 - FTP
 - IPSec
 - PPTP
- 16) Какой протокол не участвует в функционировании прикладного шлюза МЭ?
- HTTP
 - FTP
 - Telnet
 - IPSec
- 17) Какая техническая реализация VPN осуществляет шифрование специализированными микросхемами?
- На основе маршрутизаторов
 - На основе межсетевых экранов
 - 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

7.2.3 Примерный перечень заданий для решения прикладных задач (минимум 10 вопросов для тестирования с вариантами ответов)

7.2.4 Примерный перечень вопросов для подготовки к зачету

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-ЛаПаддулы.

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

7.2.5 Примерный перечень вопросов для экзамена

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. Методика выставления оценки при проведении промежуточной аттестации

(Зачет экзамена проводится по тест-билетам, каждый из которых содержит 10 вопросов к задаче. Каждый правильный ответ на вопрос тестом оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верно решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№п/п	Контролируемые разделы(темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
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. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методике выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методике выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач

чек экзаменатором и выставляется оценка, согласно методике выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практики осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНОМЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

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.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень литературы и программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

<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/> (ЭБС IPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

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

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Удалённый и непосредственный несанкционированный доступ в распределённых компьютерных системах» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны в своё время установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать 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 удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	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, ознакомиться с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению 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 промежуточной аттестации.
Подготовка к промежуточной аттестации	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.