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
«Информационные операции и атаки в распределённых информационных системах»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ / Плотников Д.Г./

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

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины– формирование у студентов системы знаний, умений и навыков в области противодействия информационным операциям и атакам в распределённых информационных системах в соответствии с Доктриной информационной безопасности Российской Федерации.

1.2.Задачиосвоениядисциплины

- ознакомить студентов с основными положениями Доктрины информационной безопасности Российской Федерации;
- дать возможность слушателям изучить средства информационного противоборства в технической и в психологических сферах, а также способов их применения в современных информационных войнах;
- способствовать, при изучении дисциплины, получению навыков формирования актуальной модели угроз для АИС и учитывать её положения при формировании требований ТЗ напроектируемую систему обеспечения ИБ;
- научить формализовывать математическая модель оценки рисков информационной безопасности автоматизированных систем при угрозах операций и атак в распределённых информационных системах;
- дать студентам представления о методах и методиках оценивания безопасности компьютерных систем при проведении аудита системы защиты;
- приобрести студентами практических навыков инструментального мониторинга защищенности компьютерных систем;
- сформировать знания и умения в области поиска рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения;
- обеспечить получение навыков установки, настройка, эксплуатации и обслуживания аппаратно-программных средств защиты информации;
- расширение области знаний по обеспечению эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности компьютерной системы.

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Информационныеоперацииииатакираспределённыхинформационныхсистемах»относитсякдисциплинамвариативнойчастиблокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Информационныеоперацииииатакираспределённыхинформационныхсистемах»направленаформированиеследующихкомпетенций:

ПК-14-способностьюпроводитьконтрольныепроверкиработоспособностиприменяемыхпрограммно-аппаратных,криптографическихитехническихсредствзащитыинформации;

ПСК-7.2-способностьюпроводитьанализрисковинформационнойбезопасностииразрабатывать,руководитьразработкойполитикибезопасностираспре

деленныхинформационныхсистемах;

ПСК-7.4-способностьюпроводитьудаленноеадминистрированиеоперационныхсистемисистембазданныхвраспределенныхинформационныхсистемах;

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ПК-14	знать принципы организации и содержание технического обслуживания технических средств и систем защиты распределённых информационных систем в контексте возможности осуществления информационных операции и атак
	уметьиспользовать средства мониторинга работоспособности и эффективностиприменяемых средств защиты распределённых информационныхв контексте возможности осуществления информационных операции и атак
	владетьметодами проверки работоспособности системы защиты информации и методами контроля соответствия конфигурации системы защитыинформации автоматизированной системы ее эксплуатационной документации
ПСК-7.2	знать методы анализа рисков информационной безопасности и разрабатывать политики безопасности в контексте возможности осуществления информационных операции и атак
	уметьразрабатывать, руководить разработкой политики безопасности в распределенных информационных системах
ПСК-7.4	знатьвиды политик управления доступом и информационными потоками в компьютерных сетях
	уметьпроводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах в контексте возможности осуществления информационных операции и атак
	владетьнавыками управления средствами межсетевого экранирования и установки программно-аппаратных средств защиты в компьютерных сетях в контексте возможности осуществления информационных операции и атак

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Информационныеоперацииииатакивраспределённыхинформационныхсистемах»составляет12з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Виды учебной работы	Всего часов	Семестры			
		6	7	8	9
Аудиторные занятия (всего)	172	40	36	36	60
В том числе:					
Лекции	76	20	18	18	20
Практические занятия (ПЗ)	96	20	18	18	40
Самостоятельная работа	188	68	54	36	30
Курсовой проект	+				+
Часы на контроль	72	-	-	36	36
Виды промежуточной аттестации - экзамен, зачет, зачет с оценкой	+	+	+	+	+
Общая трудоемкость: академические часы зач.ед.	432 12	108 3	90 2.5	108 3	126 3.5

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1	Национальные интересы Российской Федерации в информационной сфере. Социотехнические системы: информационные операции и обеспечение безопасности	Основные информационные угрозы и состояние информационной безопасности Стратегические цели и основные направления обеспечения информационной безопасности Организационные основы обеспечения информационной безопасности. Безопасность систем и информационные операции: понятийный аппарат. Управление социотехническими системами в контексте необходимости обеспечения их информационной безопасности. Методология исследования информационных операций и атак с учетом особенностей социотехнических систем	14	16	30	60
2	Типы, примеры и обнаружение атак	Понятие и классификация атак (по целям, характеру, наличию обратной связи с атакуемым объектом, по условию начала осуществления воздействия, по расположению субъекта атаки относительно атакуемого объекта, по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие) на компьютерные сети. Основные типы сетевых атак (Активные виды компьютерных атак: вирус,Root Kit,Trojan, червь.Пассивные виды атак: подслушивание, парольные атаки, скомпрометированный ключ атаки, имитация удостоверения, Application Layer атаки.) Средства реализации атак. Механизмы	14	16	30	60

		типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.				
3	Информационно-психологические операции: анализ и противодействие в отношении деструктивных технологий неформальных организаций	Простейшие операции информационно-психологического управления. Информационные операции, реализуемые неформальными объединениями и деструктивными культами. Информационные операции в рамках политических технологий. Моделирование информационно-психологических операций.	12	16	32	60
4	Террористические информационные операции	Анализ мотивов террористической деятельности на основе теории конфликта. Специфика информационных операций террористического характера. Меры противодействия террористическим атакам	12	16	32	60
5	Математическое моделирование информационных атак на ресурсы автоматизированных систем	Формальное описание модели информационных атак. Особенности использования разработанной математической модели информационных атак Математическая модель процесса обнаружения информационных атак. Математическая модель процесса оценки рисков информационной.безопасности автоматизированных систем. Описание модели процесса оценки рисков информационной безопасности. Особенности использования модели оценки рисков безопасности. Методика разработки рекомендаций по повышению уровня защиты автоматизированных систем на основе модели оценки рисков безопасности	12	16	32	60
6	Аудит информационной безопасности в компьютерных сетях	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности. Определение структуры информационно-телекоммуникационных сетей. Программные средства анализа топологии	12	16	32	60

		вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети. Средстваиметодывыявленияуязвимостейвпрограммномобеспеченииузловкомпьютернойсети. Цели и принципы зондирования узлов сети. Использованиекоммерческихисвободнораспространяемыхсредстваудитабезопасностикомпьютерныхсистем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений. Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности. Учет структуры аппаратно-программных средств объекта информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков.				
		Итого	**76**	**96**	**188**	**360**

5.2Переченьлабораторныхработ

Непредусмотреноучебнымпланом

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 8 семестре для очной формы обучения.

Примерная тематика курсового проекта: «Имитационные модели функционирования различных элементов защищенных автоматизированных систем в условиях атаки типа Denial of service».

Задачи, решаемые при выполнении курсового проекта:

1. Провести оценку функции ущерба реализации атак на компоненты информационной системы путем анализа влияния параметров системы на размер ущерба реализации атаки с целью дальнейшего управления защищенностью.

2. Произвести оценку риска реализации атак и защищенности информационной системы.

3. Разработать рекомендаций по повышению защищенности и алгоритм управления функцией защищенности, отражающий влияние методов защиты информации и мероприятий по снижению риска реализации атак в

информационных системах.

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

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениванияикомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-14	знать принципы организации и содержание технического обслуживания технических средств и систем защиты распределённых информационных систем в контексте возможности осуществления информационных операции и атак	знание принципов организации и содержание технического обслуживания технических средств и систем защиты распределённых информационных систем в контексте возможности осуществления информационных операции и атак	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметьиспользовать средства мониторинга работоспособности и эффективности применяемых средств защиты распределённых информационных в контексте возможности осуществления информационных операции и атак	умениеиспользовать средства мониторинга работоспособности и эффективности применяемых средств защиты распределённых информационных в контексте возможности осуществления информационных операции и атак	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методами проверки работоспособности системы	владение методами проверки работоспособности системы защиты информации и методами контроля соответствия конфигурации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	защиты информации и методами контроля соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	системы защиты информации автоматизированной системы ее эксплуатационной документации		
ПСК-7.2	знать методы анализа рисков информационной безопасности и разрабатывать политики безопасности в контексте возможности осуществления информационных операции и атак	знание методов анализа рисков информационной безопасности и разрабатывать политики безопасности в контексте возможности осуществления информационных операции и атак	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	умение разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-7.4	знатьвиды политик управления доступом и информационными потоками в компьютерных сетях	знаниевидов политик управления доступом и информационными потоками в компьютерных сетях	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметьпроводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах в контексте возможности осуществления информационных операции и	умениепроводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах в контексте возможности осуществления информационных операции и атак	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	атак			
	владетьнавыками управления средствами межсетевого экранирования и установки программно-аппаратных средств защиты в компьютерных сетях в контексте возможности осуществления информационных операции и атак	владениенавыками управления средствами межсетевого экранирования и установки программно-аппаратных средств защиты в компьютерных сетях в контексте возможности осуществления информационных операции и атак	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв6,7,8,9семестредляочнойформыобученияподвух/четырехбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения,характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Незачтено
ПК-14	знать принципы организации и содержание технического обслуживания технических средств и систем защиты распределённых информационных систем в контексте возможности осуществления информационных операции и атак	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметьиспользовать средства мониторинга работоспособности и эффективности применяемых средств защиты распределённых информационных в контексте возможности осуществления	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

	информационных операции и атак			
	владеть методами проверки работоспособности системы защиты информации и методами контроля соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	Решение прикладных задач в конкретной предметной области	Продемонстрирована верный ход решения в большинстве задач	Задачи не решены
ПСК-7.2	знать методы анализа рисков информационной безопасности и разрабатывать политики безопасности в контексте возможности осуществления информационных операции и атак	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	Решение стандартных практических задач	Продемонстрирована верный ход решения в большинстве задач	Задачи не решены
ПСК-7.4	знатьвиды политик управления доступом и информационными потоками в компьютерных сетях	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметьпроводить удаленное администрирование операционных систем и систем баз данных в	Решение стандартных практических задач	Продемонстрирована верный ход решения в большинстве задач	Задачи не решены

	распределенных информационных системах в контексте возможности осуществления информационных операции и атак			
	владетьнавыками управления средствами межсетевого экранирования и установки программно-аппаратных средств защиты в компьютерных сетях в контексте возможности осуществления информационных операции и атак	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

или
«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компе-тенция	**Результатыобучения,характеризующие сформированностькомпетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ПК-14	знать принципы организации и содержание технического обслуживания технических средств и систем защиты распределённых информационных систем в контексте возможности осуществления информационных операции и атак	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметьиспользовать средства	Решение стандартн	Задачи решены в полном объеме и	Продемонстр ирован верный ход решения	Продемонстр	Задачи не решены

	мониторинга работоспособности и эффективности применяемых средств защиты распределённых информационных в контексте возможности осуществления информационных операции и атак	ых практических задач	получены верные ответы	всех, но не получен верный ответ во всех задачах	ирован верный ход решения в большинстве задач	
	владеть методами проверки работоспособности системы защиты информации и методами контроля соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПСК-7.2	знать методы анализа рисков информационной безопасности и разрабатывать политики безопасности в контексте возможности осуществления информационных операции и атак	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь разрабатывать, руководить разработкой политики безопасности в	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинс	Задачи не решены

	распределенных информационных системах				тве задач	
ПСК-7.4	знатьвиды политик управления доступом и информационными потоками в компьютерных сетях	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметьпроводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах в контексте возможности осуществления информационных операции и атак	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владетьнавыками управления средствами межсетевого экранирования и установки программно-аппаратных средств защиты в компьютерных сетях в контексте возможности осуществления информационных операции и атак	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилиныематериалы,необходимыедляоценкизнаний,умений,навыковили(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1. Основная масса угроз информационной безопасности приходится на:

а) Троянские программы +

б) Шпионские программы

в) Черви

2. Какой вид идентификации и аутентификации получил наибольшее распространение:
а) системы PKI
б) постоянные пароли +
в) одноразовые пароли

3. Под какие системы распространение вирусов происходит наиболее динамично:
а) Windows
б) Mac OS
в) Android +

4. Заключительным этапом построения системы защиты является:
а) сопровождение +
б) планирование
в) анализ уязвимых мест

5. Какие угрозы безопасности информации являются преднамеренными:
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ +

6. Какой подход к обеспечению безопасности имеет место:
а) теоретический
б) комплексный +
в) логический

7. Системой криптографической защиты информации является:
а) BFox Pro
б) CAudit Pro
в) Крипто Про +

8. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы +
б) троянцы
в) черви

9. Stuxnet – это:
а) троянская программа
б) макровирус
в) промышленный вирус +

10. Таргетированная атака – это:
а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия +
в) атака на конкретный компьютер пользователя

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач
(минимум10вопросовдлятестированиясвариантамиответов)
7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач
(минимум10вопросовдлятестированиясвариантамиответов)
7.2.4Примерныйпереченьвопросовдляподготовкикзачету

Укажитевопросыдлязачета

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

Укажитевопросыдляэкзамена

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

(Например:Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5баллов заверныйответ).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	Национальные интересы Российской Федерации в информационной сфере. Социотехнические системы: информационныеоперации и обеспечение безопасности	ПК-14, ПСК-7.2, ПСК-7.4	Тест, требования к курсовому проекту
2	Типы, примеры и обнаружение атак	ПК-14, ПСК-7.2, ПСК-7.4	Тест, требования к курсовому проекту
3	Информационно-психологические операции: анализ и противодействие в отношении деструктивных технологий неформальных организаций	ПК-14, ПСК-7.2, ПСК-7.4	Тест, требования к курсовому проекту
4	Террористические информационные операции	ПК-14, ПСК-7.2, ПСК-7.4	Тест, требования к курсовому проекту
5	Математическое моделирование информационных атак на ресурсы автоматизированных систем	ПК-14, ПСК-7.2, ПСК-7.4	Тест, требования к курсовому проекту
6	Аудит информационной безопасности в	ПК-14, ПСК-7.2, ПСК-7.4	Тест, требования к курсовому проекту

	компьютерных сетях		

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

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

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценки припроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменатором,ивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампрактикосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымвметодическихматериалах.Примерноевремязащитынаодногостудентасоставляет20мин.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература

1. Белоножкин, В.И. Системы обнаружения компьютерных атак [Электронный ресурс] : Учеб.пособие. - Электрон.текстовые, граф. дан. (3,18 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.

2. Атакуемые взвешенные сети [Текст] / под ред. Д. А. Новикова. - Москва : Горячая линия - Телеком, 2018. - 247 с. : ил. - (Теория сетевых войн. № 2). - Библиогр.: с. 201-213 (214 назв.). - ISBN 978-5-9912-0684-6 : 708-00.

3. Остапенко А.Г.Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс] : Учеб.пособие. - Электрон.текстовые, граф. дан. (112 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

Дополнительная литература

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон.текстовые данные.— Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/52209.html.— ЭБС

«IPRbooks»

2. Управление информационными рисками при атаках на АСУ ТП критически важных объектов [Электронный ресурс] : Учеб.пособие. - Электрон.текстовые, граф. дан. (544 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

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

https://www.snort.org/downloads
http://www.winroute.ru
http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
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«Информационныеоперациииатакираспределённыхинформационныхсистемах»читаютсялекции,проводятсяпрактическиезанятия,выполняетсякурсовойпроект.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Практическиезанятия (примерные темы).

1.Создание защищенныхсегментовприработевсети Интернетсиспользованиеммежсетевыхэкранов. Применениефильтрующегомаршрутизатора WinRoute

2.ПрименениеСОА Snort дляобнаруженияскрытогосканирования, атак, использующихпреднамеренноенарушениеструктурысетевыхпакетов,

атаквида«отказвобслуживании».

3.Применениетехнологииинтерминальногодоступа.

4.Применениепрограммныхсредства аудитаинформационнойбезопасностисцельютестированиясостоянияз ащищенностикомпьютерныхсистемотнесанкционированногодоступа и выработкимерзащитыотвыявленныхугроз.Занятияпроводятсяпутемрешения конкретныхзадачваудитории.

Методикавыполнениякурсовогопроектаизложенавучебно-методическом пособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременноиустановленныесроки.

Контрольусвоенияматериладисциплиныпроизводитсяпроверкойкурсовогопроекта,защитойкурсовогопроекта.

Вид учебных занятий	Деятельность студента
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.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	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 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, зачетом с оценкой, экзаменом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.