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

«Оценка эффективности противодействия ИОА в РКС»

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

Целью изучения дисциплины является изучение основных аспектов оценки эффективности противодействия информационных операций и атак в распределенных компьютерных системах и овладение основными методами проведения данного анализа на основе отечественных и зарубежных стандартов в области компьютерной безопасности.

1.2. Задачи освоения дисциплины

- изучение методов оценки противодействия ИОА в РКС на основе регламентирующих документов
- изучение общих принципов построения подсистемы информационной безопасности в распределенных компьютерных системах с учетом оценки эффективности противодействия ИОА в РКС

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«ОценкаэффективностипротиводействияИОАвРКС»относитсякдисциплинамвариативнойчасти(дисциплинаповыбору)блокаБ1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Оценкаэффективностипротиводействия ИОАвРКС»направленаформированиеследующихкомпетенций:

ПК-16-способностьюразрабатыватьпроектынормативныхправовыхактоваметодическиематериалы,регламентирующиеработупообеспечениюинформационнойбезопасностикомпьютерныхсистем

ПК-20-способностьювыполнятьработыповосстановлениюработоспособностисредствзащитыинформациипривозникновенииинештатныхситуаций

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ПК-16	Знать нормативно-правовые документы, регламентирующие работу по наладке и настройке программно-аппаратных систем защиты распределенных компьютерных систем
	Уметь применять современные системы управления и принятия решения по защитев распределенных компьютерных систем
	Владетьнавыками анализа основных характеристик и возможностей информационных операций и атак в распределенных компьютерных систем
ПК-20	Знать основные методы оценки надежности механизмов защиты

	информациив распределенных компьютерных систем
	Уметьанализировать применяемые механизмы защиты информации в распределенных компьютерных системах, а такжеоценивать степень надежность применяемых механизмов защиты информации.
	Владетьмеханизмами обеспечения безопасности и методами оценки надежности механизмов защиты информации в распределенных компьютерных систем**.**

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Оценкаэффективностипротиводействия ИОАвРКС»составляет7з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всего часов	Семестры	
		9	10
Аудиторныезанятия (всего)	90	54	36
В томчисле:			
Лекции	54	36	18
Лабораторныеработы (ЛР)	36	18	18
Самостоятельнаяработа	126	36	90
Курсовойпроект	+		+
Часынаконтроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 252 7	 90 2.5	 162 4.5

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. зан.	СРС	Всего,

						час
1	Постановка задачи анализа защищенности компьютерной системы	РКС как объект защиты; понятие и классификация уязвимостей; Уязвимости и безопасность промышленных систем управления ; Основные приемы выявления уязвимостей; Системы анализа защищенности;Размещение сетевых агентов сканирования в сети ;Идентификация узлов с помощью протокола ARP ;Использование протокола ICMP при идентификации узлов всети;Отслеживание маршрутов и фильтрация;Утилита traceproto; Сканирование портов TCP; Методы идентификации уязвимостей по косвенным признакам	10	6	20	36
2	Методология анализа защищенности и уровня эффективности противодействия атакам	Сетевой сканерNessus: архитектура, обзорвозможностей; ЯзыкописанияатакNASL; СканерыбезопасностикомпанииPositiveTechnologies; Архитектураиосновныевозможностисканера XSpider; Методологияанализазащищенностиethical Hacking; СтруктураPenetrationTesting	10	6	20	36

	Итого за 9-ый семестр		36	18	36	90
3	Источники данных для систем обнаружения атак	Сетевой трафик как источник данных; Host IDS — контроль действий субъектов системы; Использование известных техник и инструментов для проведения атак; Система обнаружения атак Snort; Интеграция средств обнаружения и предотвращения атак в единую систему	10	6	20	36
4	Методыоценивания информационныхр исков	Анализ методики CRAMM; Анализ методики FRAP; Анализ методики RiskWatch; Анализ методики Гриф; Разработка методики оценки рисков на примере методики Microsoft;Математические модели оценки эффективности противодействия информационным операциям и атакам	8	6	22	36
		Итого 10-ый семестр	**18**	**18**	**90**	**126**
		Итого	**54**	**36**	**126**	**216**

5.2Перечеьлабораторныхработ

Неделя семестра	Наименованиелабораторнойработы	Объем часов	В том числе в интерактивной форме (ИФ)	Вид контр
9-ый семестр		**18**	**-**	
	Знакомство с отечественными руководящими документами в области компьютерной безопасности	4		отчет
	Знакомство с иностранными руководящими документами в области компьютерной безопасности	4		отчет
	Определение пар угроза-уязвимость при осуществлении типовых ИОА на	4		отчет

	РКС			
	Построение математических моделей ИОА в РКС	6		отчет
Итогоза 9-ый семестр		18		
10-ый семестр		18		
	Определение оптимального набора средств противодействия ИОА в РКС	4		отчет
	Численная оценка эффективности противодействия ИОА в РКС	4		отчет
	Оценка эффективности противодействия ИОА в РКС на основе экспертных оценок.	2		отчет
	Построение подсистемы информационной безопасности в распределенных компьютерных системах с учетом оценки эффективности противодействия ИОА.	4		отчет
	Оптимизация подсистемы информационной безопасности в РКС с учетом оценки эффективности противодействия ИОА.	4		отчет
Итогоза10-ый семестр		**18**		
	Итого	**36**		

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплиныпредусматриваетвыполнениекурсовыхпроектовв10семестрахдляочнойформыобучения.

Примернаятематикакурсовогопроекта:«Моделирование систем оценки эффективности противодействия информационным операциям и атакам»(по вариантам)

Курсовойпроектвключатвсебяграфическуючастьирасчетно-пояснительнуюзаписку.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениванияикомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестациионениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующиесформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-16	Знать нормативно-правовые документы, регламентирующие работу по наладке и настройке программно-аппаратных систем защиты распределенных компьютерных систем	Знание нормативно-правовые документы, регламентирующие работу по наладке и настройке программно-аппаратных систем защиты распределенных компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь применять современные системы управления и принятия решения по защите в распределенных компьютерных систем	Умение применять современные системы управления и принятия решения по защите в распределенных компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками анализа основных характеристик и возможностей информационных операций и атак в распределенных компьютерных систем	Владение навыками анализа основных характеристик и возможностей информационных операций и атак в распределенных компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-20	Знать основные методы оценки надежности механизмов защиты информации в распределенных компьютерных систем	Знание основныч методов оценки надежности механизмов защиты информации в распределенных компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь анализировать применяемые механизмы защиты информации в распределенных компьютерных системах, а также оценивать степень надежность применяемых механизмов защиты информации.	Умение анализировать применяемые механизмы защиты информации в распределенных компьютерных системах, а также оценивать степень надежность применяемых механизмов защиты информации.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	Владеть механизмами обеспечения безопасности и методами оценки надежности механизмов защиты информации в распределенных компьютерных системах.	Владениемеханизмами обеспечения безопасности и методами оценки надежности механизмов защиты информации в распределенных компьютерных системах.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв9,10семестре дляочнойформыобученияподвух/четырехбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
ПК-16	Знать нормативно-правовые документы, регламентирующие работу по наладке и настройке программно-аппаратных систем защиты распределенных компьютерных систем	Тест	Выполнениестана 70-100%	Выполнение менее 70%
	Уметь применять современные системы управления и принятия решения по защите в распределенных компьютерных систем	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	Владеть навыками анализа основных характеристик и возможностей информационных операций и атак в распределенных компьютерных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПК-20	Знать основные методы оценки надежности механизмов защиты информации в распределенных компьютерных систем	Тест	Выполнениестана 70-100%	Выполнение менее 70%
	Уметь анализировать	Решениестандартныхпрактическихзадач	Продемонстрирова н верный	Задачинерешены

	применяемые механизмы защиты информации в распределенных компьютерных системах, а также оценивать степень надежность применяемых механизмов защиты информации.		ход решения в большинстве задач	
	Владеть механизмами обеспечения безопасности и методами оценки надежности механизмов защиты информации в распределенных компьютерных систем**.**	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены

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

Компе-тенция	**Результатыобучения ,характеризующие сформированностьк омпетенции**	**Критерии оценивания**	**Отличн о**	**Хорошо**	**Удовл.**	**Неудов л.**
ПК-16	Знать нормативно-правовые документы, регламентирующие работу по наладке и настройке программно-аппаратных систем защиты распределенных компьютерных систем	Тест	Выполнениетеста на 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	Уметь применять современные системы управления и принятия решения по защите в распределенных компьютерных систем	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачинерешены
	Владеть навыками анализа основных характеристик и	Решение прикладных задач в конкретной	Задачи решены в полном объеме и	Продемонстрирован верный ход решения	Продемонстрирован верный ход	Задачинерешены

	возможностей информационных операций и атак в распределенных компьютерных систем	предметной области	получены верные ответы	всех, но не получен верный ответ во всех задачах	решения в большинстве задач	
ПК-20	Знать основные методы оценки надежности механизмов защиты информации в распределенных компьютерных систем	Тест	Выполнениетеста на 90-100%	Выполнениетестана 80- 90%	Выполнениетестана 70- 80%	В тесте менее 70% правильных ответов
	Уметь анализировать применяемые механизмы защиты информации в распределенных компьютерных системах, а также оценивать степень надежность применяемых механизмов защиты информации.	Решениестандартныхпрактическихзадач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
	Владеть механизмами обеспечения безопасности и методами оценки надежности механизмов защиты информации в распределенных компьютерных систем**.**	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены

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

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1. Что такое сертификация средств защиты информации согласно российскому законодательству?

а) подтверждение соответствия заявленных и фактических технических характеристик в области ИБ для приложений, компьютерных систем, инфраструктуры

б) комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации

в) разрешение использования информационной системы общего применения или специализированных приложений (имеющих специальные требования к ИБ) для обработки

информации

г) деятельность, позволяющая убедиться в их соответствии требованиям государственных стандартов или иных нормативных документов по защите информации

2. К какому подходу по управлению рисками относится страхование оборудования от выхода из строя?

а) уменьшение риска

б) уклонение от риска

в) изменение характера риска

г) принятие риска

3. Как называется информационный ресурс, от которого зависит ряд важных задач, но в случае утраты он может быть восстановлен за время, не превышающее критически допустимое, но стоимость восстановления – высокая?

а) малоценный информационный ресурс

б) ресурс средней ценности

в) ценный ресурс

г) особо ценный ресурс

4. Кто проводит аудит ИБ?

а) команда специалистов по безопасности корпоративных систем и специалистов в области менеджмента

б) команда специалистов верхнего уровня в области информационной безопасности

в) команда специалистов в сфере сертификации ИБ

г) команда специалистов по обслуживанию систем ИБ

5. Что понимается под субъективной вероятностью?

а) вероятностные распределение на множестве событий

б) мера уверенности некоторого человека или группы людей в том, что данное событие в действительности будет иметь место

в) относительная частота появления какого-либо события в общем объеме наблюдений или отношение числа благоприятных исходов к общему количеству наблюдений

г) мера уверенности на множестве событий, отражающая предпочтительный вариант из множества альтернатив

6. Как кодируется происшествие с умеренными результатами?

а) N

б) Mi

в) S

г) Mo

7. Информационные риски компании не зависят от:

а) показателей ценности информационных ресурсов

б) вероятности реализации угроз для ресурсов

в) количества ресурсов

г) эффективности существующих или планируемых средств обеспечения информационной безопасности

8. Какой параметр не идентифицирует риск?

а) степень разрушительности воздействия на ресурс, выражаемой в виде коэффициента разрушительности

б) угроза, возможной реализацией которой вызван данный риск;

в) ресурс, в отношении которого может быть реализована данная

г) уязвимость, через которую может быть реализована данная угроза в отношении данного ресурса

9. От какого риска возможно уклониться?

а) инсайдер внутри компании

б) несанкционированный доступ в локальную сеть со стороны Web-клиентов

в) уязвимости в программном обеспечении

г) атаки типа «отказ в обслуживании»

10. Что не входит в план оценки информационных рисков компании?

а) Идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса.

б) Оценивание возможных угроз

в) Оценивание информационных рисков от существующих конкурентов

г) Оценивание эффективности средств обеспечения информационной безопасности

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

1. Какому уровню зрелости управления рисками безопасности согласно методикиMicrosoft соответствует глубокое понимание управления рисками на всех уровнях организации?

а) оптимизированный

б) наличие определенного процесса

в) управляемый

г) узкоспециализированный

2. К какой группе требований согласно спецификацийXBSS относится требование, что когда пользовательский сеанс приостановлен (блокирован), вывод также необходимо приостановить, а экран монитора погасить?

а) Требования к подсистеме идентификации и аутентификации

б) Требования к защите критичной информации

в) Требования к подсистеме управления доступом

г) Требования к средствам управления ИБ

3. К какой фазе жизненного цикла информационной технологии согласно стандарта NIST 800-30 относится выявление рисков, специфичных для данной ИС?

а) Создание ИС

б) Предпроектная стадия

в) Проектирование ИС

г) Функционирование ИС

4. Какая группа отечественных заказчиков работ в области защиты информации предлагает проектировщикам выполнить полный цикл работ, начиная с анализа рисков и кончая системой поддержания режима информационной безопасности на всех стадиях жизненного цикла?

а) государственные структуры

б) коммерческие структуры с настоящими собственниками информационных ресурсов компании

в) коммерческие структуры с формальными собственниками информационных ресурсов компании

г) структуры, для которых обязательно соответствие зарубежным стандартам в

области информационной безопасности

5. На каком этапе RiskAdvisor анализирует сильные и слабые стороны организации с внешних позиций, варианты развития, классы угроз и отношения с партнерами?

а) Описание контекста

б) Описание угроз

в) Описание рисков

г) Описание потерь

6. К какой оценке уровня риска согласно методикиFRAP относится описание «требуется мониторинг ситуации»?

а) уровень D

б) уровень A

в) уровень C

г) уровень B

7. В каком разделе стандарта BS 7799 одной из целей является обеспечение надлежащего уровня защиты информационных ресурсов?

а) Политика ИБ

б) Организация защиты

в) Администрирование информационных систем

г) Классификация ресурсов и их контроль

8. Какой уровень стойкости согласно стандартаISO 15408 означает, что функция обеспечивает адекватную защиту от случайного нарушения безопасности ОО нарушителем с низким потенциалом нападения?

а) Низкая стойкость

б) Базовая стойкость

в) Средняя стойкость

г) Высокая стойкость

9. Какого типа источника угроз нет в стандарте OCTAVE?

а) угрозы, связанные с правоохранительными органами

б) угрозы, исходящие от человека-нарушителя, действующего через сеть передачи данных

в) угрозы, исходящие от человека-нарушителя, использующего физический доступ

г) угрозы, связанные со сбоями в работе системы

10. Какой компонент в системе SymantecEnterpriseSecurityManager осуществляет управление данными о результатах выполненных проверок?

а) Агент ESM

б) Модули политики безопасности ESM

в) Менеджер ESM

г) Модули запросов

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

1.РКС как объект защиты;

2. Понятие и классификация уязвимостей;

3. Уязвимости и безопасность промышленных систем управления;

4. Основные приемы выявления уязвимостей;

5. Системы анализа защищенности;
6. Размещение сетевых агентов сканирования в сети;
7.Идентификация узлов с помощью протокола ARP;
8. Использование протокола ICMP при идентификации узлов всети;
9. Отслеживание маршрутов и фильтрация;
10. Утилита traceproto;
11. Сканирование портов TCP;
12. Методы идентификации уязвимостей по косвенным признакам
13.Сетевой сканер Nessus: архитектура, обзор возможностей;
14. Язык описания атак NASL;
15. Сканеры безопасности компании PositiveTechnologies;
16. Архитектура и основные возможности сканера XSpider;
17.Методология анализа защищенности EthicalHacking;
18. Структура PenetrationTesting
19. Сетевой трафик как источник данных;
20. HostIDS — контроль действий субъектов системы;
21. Использование известных техник и инструментов для проведения атак;

22. Интеграция средств обнаружения и предотвращения атак
в единую систему
23. Анализ методики CRAMM;
24. Анализ методики FRAP;
25. Анализ методики RiskWatch;
26. Анализ методики Гриф;
27. Разработка методики оценки рисков на примере методики Microsoft;
28. Математические модели оценки эффективности противодействия информационным операциям и атакам
29.Система обнаружения атак Snort.

7.2.5Примерныйпереченьзаданийдляэкзамена

1.РКС как объект защиты;
2. Понятие и классификация уязвимостей;
3. Уязвимости и безопасность промышленных систем управления;
4. Основные приемы выявления уязвимостей;
5. Системы анализа защищенности;
6. Размещение сетевых агентов сканирования в сети;
7.Идентификация узлов с помощью протокола ARP;
8. Использование протокола ICMP при идентификации узлов всети;
9. Отслеживание маршрутов и фильтрация;
10. Утилита traceproto;
11. Сканирование портов TCP;
12. Методы идентификации уязвимостей по косвенным признакам
13.Сетевой сканер Nessus: архитектура, обзор возможностей;
14. Язык описания атак NASL;
15. Сканеры безопасности компании PositiveTechnologies;
16. Архитектура и основные возможности сканера XSpider;
17.Методология анализа защищенности EthicalHacking;
18. Структура PenetrationTesting
19. Сетевой трафик как источник данных;
20. HostIDS — контроль действий субъектов системы;
21. Использование известных техник и инструментов для проведения атак;

22. Интеграция средств обнаружения и предотвращения атак

в единую систему

23. Анализ методики CRAMM;

24. Анализ методики FRAP;

25. Анализ методики RiskWatch;

26. Анализ методики Гриф;

27. Разработка методики оценки рисков на примере методики Microsoft;

28. Математические модели оценки эффективности противодействия информационным операциям и атакам

29.Система обнаружения атак Snort.

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

(Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит10 вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1ба ллом,задачаоценивается в10баллов(5балловверноерешениеи5балловзаверныйо твет).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабра лменее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабрало т6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15балл ов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы)дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Постановка задачи анализа защищенности компьютерной системы	ПК-16, ПК-20	Тест, контрольная работа, защита лабораторных работ, защита реферата,
2	Методология анализа защищенности и уровня эффективности противодействия атакам	ПК-16, ПК-20	Тест, контрольная работа, защита лабораторных работ, защита реферата,
3	Источники данных для систем обнаружения атак	ПК-16, ПК-20	Тест, контрольная работа, защита лабораторных работ, защита реферата,
4	Методыоцениванияинформационныхрисков	ПК-16, ПК-20	Тест, контрольная работа, защита лабораторных работ, защита реферата,

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

Тестированиеосуществляется,либоприпомощикомпьютернойсистемыт

естирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампрактикосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымвметодическихматериалах.Примерноевремязащитынаодногостудентасоставляет20мин.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

1. Гончаров И.В. Технические средства обеспечения информационной безопасности [Электронный ресурс]: Учеб. пособие / И. В. Гончаров. - Электрон. текстовые, граф. дан. (355 Кб). - Воронеж: ГОУВПО "Воронежский государственный технический университет", 2009. - 1 файл. - 30-00.0.
2. Иванкин Е.Ф. Основы теории информации и их применение в риск-анализе информационных систем [Электронный ресурс]: Учеб. пособие / Е. Ф. Иванкин, М. П. Иванкин. - Электрон. текстовые, граф. дан. (2047 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 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.

Дополнительная литература:

1. Методические указания к самостоятельным работам по дисциплинам «Информационные операции и атаки в

распределенных компьютерных системах», «Оценка эффективности противодействия ИОА в РКС», «Информационные операции и атаки в распределенных информационных системах» для студентов специальностей 090301 «Компьютерная безопасность», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Е. С. Соколова, Д. Г. Плотников. - Электрон. текстовые, граф. дан. (451 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 00-00.

2. Оптимальный синтез и анализ эффективности комплексов защиты информации: Монография / В. Г. Кулаков [и др.]. - Воронеж: ВГТУ, 2006. - 137 с. - 30-00.
3. Информационные операции [Электронный ресурс]: учеб. пособие / Г. А. Остапенко, Е. А. Мешкова. - Электрон. дан. (1 файл :3045 Кбайта). - Воронеж: ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.

8.2Переченьинформационныхтехнологий,используемыхприосуществлениииобразовательногопроцессаподисциплине,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«ОценкаэффективностипротиводействияИОАвРКС»читаютсялекции,проводятсялабораторныеработы,выполняетсякурсовойпроект.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяна

иболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Методикавыполнениякурсовогопроектаизложенавучебно-методическомпособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременноивустановленныесроки.

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.