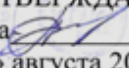


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

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

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

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. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Оценка эффективности противодействия ИОА в РКС» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Оценка эффективности противодействия ИОА в РКС» направлен на формирование следующих компетенций:

ПК-16 – способность разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем

ПК-20 – способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении инцидентов

Компетенция	Результаты обучения, характеризующие сформированность компетенции
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 защите в распределенных компьютерных системах
	Владеть навыками анализа основных характеристик и возможностей информационных операций и атак в распределенных компьютерных системах
ПК-20	Знать основные методы оценки надежности механизмов защиты информации в распределенных

	компьютерных систем
	Уметь анализировать применяемые механизмы защиты информации в распределенных компьютерных системах, а также оценивать степень надежность применяемых механизмов защиты информации.
	Владеть механизмами обеспечения безопасности и методами оценки надежности механизмов защиты информации в распределенных компьютерных систем.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Оценка эффективности противодействия ИОА ВРКС» составляет 10 з.е.

Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	144	36	108
В том числе:			
Лекции	90	18	72
Практические занятия (ПЗ)	54	18	36
Самостоятельная работа	180	54	126
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость:			
академические часы	360	90	270
зач.ед.	10	2.5	7.5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Пр. зан.	СРС	Всего, час
1	Постановка задачи	РКС как объект защиты; понятие и	10	6	20	36

	анализа защищенности компьютерной системы	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				
2	Методология анализа защищенности и уровня эффективности противодействия атакам	Сетевой сканерNessus: архитектура, обзорвозможностей; ЯзыкописанияатакNASL; СканерыбезопасностикомпанийPositiveTechnologies; АрхитектураиосновныевозможностисканераXSpider; МетодологияанализазащищенностииEthicalHacking; СтруктураPenetrationTesting	10	6	20	36
	Итого за 9-ый семестр		18	18	54	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	10	6	20	36

		атак; Система обнаружения атак Snort; Интеграция средств обнаружения и предотвращения атак в единую систему				
4	Методы оценивания информационных рисков	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			72	36	126	234
Итого			90	54	180	324

5.2 Перечень лабораторных работ

Лабораторные работы не предусмотрены

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

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовых проектов в 10 семестрах для очной формы обучения.

Примерная тематика курсового проекта: «Моделирование систем оценки эффективности противодействия информационным операциям и атакам» (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

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«неаттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-16	Знать нормативно-правовые документы, регламентирующие работу по наладке и настройке программно-аппаратных систем защиты	Знание нормативно-правовых документов, регламентирующих работу по наладке и настройке программно-аппаратных	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	распределенных компьютерных систем	систем защиты распределенных компьютерных систем		
	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 основных 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 систем.	Владение механизмами обеспечения безопасности и методами 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

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-16	Знать нормативно-правовые документы, регламентирующие работу по наладке и настройке программно-аппаратных систем защиты распределенных	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

	компьютерных систем			
	Уметь применять современные системы управления и принятия решения по защите в распределенных компьютерных систем	Решение стандартных практических задач	Продемонстрировать правильный ход решения в большинстве задач	Задача решена
ПК-20	Владеть навыками анализа основных характеристик и возможностей информационных операций и атак в распределенных компьютерных систем	Решение прикладных задач в конкретной предметной области	Продемонстрировать правильный ход решения в большинстве задач	Задача решена
	Знать основные методы оценки надежности механизмов защиты информации в распределенных компьютерных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь анализировать применяемые механизмы защиты информации в распределенных компьютерных системах, а также оценивать степень надежность применяемых механизмов защиты информации.	Решение стандартных практических задач	Продемонстрировать правильный ход решения в большинстве задач	Задача решена
	Владеть механизмами обеспечения безопасности и методами оценки надежности механизмов защиты информации в распределенных компьютерных систем.	Решение прикладных задач в конкретной предметной области	Продемонстрировать правильный ход решения в большинстве задач	Задача решена

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-16	Знать нормативно-правовые документы, регламентирующие работу по наладке и настройке программно-аппаратных систем защиты распределенных компьютерных систем	Тест	Выполнение теста 90-100%	Выполнение теста 80-90%	Выполнение теста 70-80%	В тесте менее 70% правильных ответов
	Уметь применять современные системы управления и принятия	Решение стандартных практических задач	Задачи решены в полном	Продемонстрирован правильный ход	Продемонстрирован правильный ход решения в	Задача решена

	решения по защите в распределенных компьютерных систем		объеме и получены верные ответы	решения всех, но не получен верный ответ во всех задачах	большинстве задач	
	Владеть навыками анализа основных характеристик и возможностей информационных операций и атак 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
ПК-20	Знать основные методы оценки надежности механизмов защиты информации в распределенных компьютерных систем	Тест	Выполнение теста 90-100%	Выполнение теста 80-90%	Выполнение теста 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.	Решение стандартных практических задач	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

7.2 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 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) M_i
- в) S
- г) M_o

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

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Какому уровню зрелости управления рисками безопасности согласно методики Microsoft 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 спецификаций XBSS 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 в сети;
9. Отслеживание маршрутов и фильтрация;
10. Утилита traceroute;
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 Positive Technologies;
16. Архитектура и основные возможности сканера XSpider;
17. Методология анализа защищенности Ethical Hacking;
18. Структура Penetration Testing
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.

7.2.5 Примерный перечень заданий для экзамена

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 в сети;
9. Отслеживание маршрутов и фильтрация;
10. Утилита traceroute;
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 Positive Technologies;
16. Архитектура и основные возможности сканера XSpider;
17. Методология анализа защищенности Ethical Hacking;
18. Структура Penetration Testing
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. Методика выставления оценки при проведении промежуточной аттестации

(Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос тесте 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	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	Методы оценивания информационных рисков	ПК-16, ПК-20	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 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 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

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.

8.2 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 «Оценка эффективности противодействия ИОА в РКС» 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

мпособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременновустановленныесроки.

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 удастся 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, ознакомиться 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.