РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационные операции и атаки в распределенных информационных системах

(наименование дисциплины (модуля) по УП)

Закреплена за кафедрой: систем информационной безопасности

Направление подготовки (специальности): 10.05.03 Информационная безопасность автоматизированных систем

Профиль: Обеспечение информационной безопасности распределенных информационных систем

(название профиля по УП)

Часов по УП: 396; Часов по РПД: 396;
Часов по УП (без учета часов на экзамены): 360; Часов по РПД: 360;
Часов на интерактивные формы (ИФ) обучения по УП: -
Часов на интерактивные формы (ИФ) обучения по РПД: -
Часов на самостоятельную работу по УП: 172(47,78%);
Часов на самостоятельную работу по РПД: **172 47,78%);**
Общая трудоемкость в ЗЕТ: 11;
Виды контроля в семестрах (на курсах): экзамен – 7; зачет с оценкой– 8;
Форма обучения: очная**;**
Срок обучения: нормативный**.**

Распределение часов дисциплины по семестрам

Вид занятий	**№ семестров, число учебных недель в семестрах**																	
	2 / 18		3 / 18		4 / 18		5 / 18		6 / 18		7 / 20		8 / 22		9 / 22		Итого	
	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
Лекции											54	54	40	40			94	94
Лабораторные																		
Практические											54	54	40	40			94	94
Ауд. занятия																		
Сам. работа											72	72	100	100			172	172

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	**Цель изучения дисциплины** «Информационные операции и атаки в распределенных информационных системах» - системное изучение информационных операций, реализуемых в СТС, а также вопросы обеспечения безопасности информационных пространств в условиях противодействия ИО.
1.2	**Для достижения цели ставятся задачи:**
1.2.1	Освоение способов реализации информационных операций;
1.2.2	освоение подходов противодействия ИО.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Цикл (раздел) ООП: С.3	код дисциплины в УП С3.В.ОД.1
2.1 Требования к предварительной подготовке обучающегося	
Для успешного освоения дисциплины студент должен иметь базовую подготовку по физике, информатике и математике в пределах программы средней школы, а также дисциплины младших курсов, такие как	
С2.В.ДВ.1.2	Математические модели информационного противоборства
С3.Б.18	Информационная безопасности распределённых информационных систем
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее	
С3.В.ОД.2	Социальные сети: риски и обеспечение безопасности
С3.В.ДВ.1.3	Оценка эффективности регионального информационного противоборства

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-17 ПК-18 ПК-19 ПК-20 ПК-21 ПК-22 ПК-23 ПК-24 ПК-25 ПК-26 ПК-27 ПК-28 ПК-29 ПК-30 ПК-31 ПК-32 ПК-33 ПК-34 ПК-35 ПК-36 ПК-37 ПК-38 ПК-39 ПК-40	**Знать:** - сущность и понятие, информационной безопасности и характеристику ее составляющих; -место и роль информационной безопасности в системе национальной безопасности РФ, основы государственной информационной политики, стратегию развития информационного общества в России; - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. **Уметь:** -классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; -анализировать и оценивать угрозы информационной безопасности объекта; -применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; **Владеть:** - профессиональной терминологией в области информационной безопасности; -методами формирования требований по защите информации.
ПСК-7.1 ПСК-7.2 ПСК-7.3 ПСК-7.4 ПСК-7.5 ПСК-7.6 ПСК-7.7 ПСК-7.8 ПСК-7.9	**Знать:** - основные положения теории управления; - способы обеспечения информационной безопасности систем организационного управления; **Уметь**: - разрабатывать модели систем организационного управления; **Владеть:** - навыками разработки политики безопасности систем организационного управления.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Основные способы реализации информационных операций;
3.2	**Уметь:**
3.2.1	Оказывать противодействия атакам на распределенные информационные системы
3.3	**Владеть:**
3.3.1	профессиональной терминологией в области информационной безопасности;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ п/п	Наименование раздела дисциплины	Семестр	Неделя семестра	Вид учебной нагрузки и их трудоемкость в часах				
				Лекции	Практические занятия	Лабораторные. работы	СРС	Всего часов
1	Социотехнические системы: информационные операции и обеспечение безопасности	7	1-5	14			20	**34**
2	Информационно-кибернетические операции: анализ и противодействие в отношении сетевых компьютерных атак	7	6-20	40	54		52	**146**
3	Информационно-психологические операции: анализ и противодействие в отношении деструктивных технологий неформальных организаций	8	1-13	24	10		54	**88**
4	Террористические информационные операции	8	14-22	16	30		46	**92**
Итого				**94**	**94**		**172**	**360**

4.1 Лекции

Неделя семестра	Тема и содержание лекции	Объем часов	В том числе, в интерактивной форме (ИФ)
7 семестр			
Социотехнические системы: информационные операции и обеспечение безопасности		**14**	
1-5	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 *Самостоятельное изучение.* 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	
Информационно-кибернетические операции: анализ и противодействие в отношении сетевых компьютер-		**40**	

ных атак			
6-20	Классификация сетевых угроз для информационно-телекоммуникационных систем. Атаки на основе подбора имени и пароля посредством перебора. Атаки на основе сканирования портов. Атаки на основе анализа сетевого трафика. Атаки на основе внедрения ложного доверенного объекта. Атаки на основе отказа в обслуживании. Оценка рисков кибернетических атак *Самостоятельное изучение.* Классификация сетевых угроз для информационно-телекоммуникационных систем. Атаки на основе подбора имени и пароля посредством перебора. Атаки на основе сканирования портов. Атаки на основе анализа сетевого трафика. Атаки на основе внедрения ложного доверенного объекта. Атаки на основе отказа в обслуживании. Оценка рисков кибернетических атак	40	
Итого за 7 семестр		**54**	
8 семестр			
Информационно-психологические операции: анализ и противодействие в отношении деструктивных технологий неформальных организаций		**24**	
1-13	Простейшие операции информационно-психологического управления. Информационные операции, реализуемые неформальными объединениями и деструктивными культами. Информационные операции в рамках политических технологий. Моделирование информационно-психологических операций *Самостоятельное изучение.* Простейшие операции информационно-психологического управления. Информационные операции, реализуемые неформальными объединениями и деструктивными культами. Информационные операции в рамках политических технологий. Моделирование информационно-психологических операций	24	
Террористические информационные операции		**16**	
14-22	Анализ мотивов террористической деятельности на основе теории конфликта. Специфика информационных операций террористического характера. Меры противодействия террористическим атакам *Самостоятельное изучение.* Анализ мотивов террористической деятельности на основе теории конфликта. Специфика информацион-	16	

	ных операций террористического характера. Меры противодействия террористическим атакам		
Итого за 8 семестр		**40**	
Всего		**94**	

4.2 Практические занятия

Неделя семестра	Наименование практической работы	Объем часов	В том числе в интерактивной форме (ИФ)	Виды контроля
7 семестр		**54**	**-**	
8	Атаки на основе подбора имени и пароля посредством перебора.	8		отчет
11	Атаки на основе сканирования портов	8		отчет
13	Атаки на основе анализа сетевого трафика.	8		отчет
15	Атаки на основе внедрения ложного доверенного объекта.	10		отчет
17	Атаки на основе отказа в обслуживании.	10		отчет
18	Оценка рисков кибернетических атак	10		отчет
8 семестр		**40**		отчет
10	Моделирование информационно-психологических операций	10		отчет
14	Анализ мотивов террористической деятельности на основе теории конфликта.	10		отчет
17	Специфика информационных операций террористического характера	10		отчет
20	Меры противодействия террористическим атакам	10		отчет
Всего		**94**		отчет

4.3 Лабораторные работы

Не предусмотрены

4.4 Самостоятельная работа студента (СРС)

Неделя семестра	Содержание СРС	Виды контроля	Объем часов

7 семестр		**Зачет**	**72**
1	Простейшие операции информационно-психологического управления.	Подготовка конспекта лекций, подготовка к практическому занятию.	6
3	Информационные операции, реализуемые неформальными объединениями и деструктивными культами	Подготовка конспекта лекций, подготовка к практическому занятию.	8
5	Информационные операции в рамках политических технологий.	Подготовка конспекта лекций подготовка к письменной проверочной работе по пройденному материалу. Сдача одного из этапов курсовой работы.	6
6	Классификация сетевых угроз для информационно-телекоммуникационных систем.	Подготовка конспекта лекций, подготовка к практическому занятию.	6
8	Атаки на основе подбора имени и пароля посредством перебора.	Подготовка конспекта лекций, подготовка к практическому занятию.	6
11	Атаки на основе сканирования портов	Подготовка конспекта лекций, подготовка к практическому занятию.	8
13	Атаки на основе анализа сетевого трафика.	Подготовка конспекта лекций, подготовка к практическому занятию.	8
15	Атаки на основе внедрения ложного доверенного объекта.	Подготовка конспекта лекций, подготовка к практическому занятию.	8
17	Атаки на основе отказа в обслуживании.	Подготовка конспекта лекций, подготовка к практическому занятию.	8
18	Оценка рисков кибернетических атак	Подготовка конспекта лекций подготовка к письменной проверочной работе по пройденному материалу. Сдача одного из этапов курсовой работы.	8
8 семестр		**Зачет**	**100**
1	Простейшие операции информационно-психологического управления.	Подготовка конспекта лекций, подготовка к практическому занятию.	12
4	Информационные операции, реализуемые неформальными объединениями и деструктивными культами.	Подготовка конспекта лекций, подготовка к практическому занятию.	16
8	Информационные операции в рамках политических технологий.	Подготовка конспекта лекций, подготовка к практическому занятию.	14

10	Моделирование информационно-психологических операций	Подготовка конспекта лекций подготовка к письменной проверочной работе по пройденному материалу. Сдача одного из этапов курсовой работы.	12
14	Анализ мотивов террористической деятельности на основе теории конфликта.	Подготовка конспекта лекций, подготовка к практическому занятию.	16
17	Специфика информационных операций террористического характера	Подготовка конспекта лекций, подготовка к практическому занятию.	14
20	Меры противодействия террористическим атакам	Подготовка конспекта лекций, подготовка к практическому занятию.	16

4.5 Темы курсовых работ

1. Геополитическое пространство как поле для ИО
2. Информационная война как совокупность ИО
3. Кибертерроризм как разновидность ИО
4. Глобальные трансформации
5. Ущербы и риски при ИО
6. Угрозы и опасность при ИО
7. Информационное управление как разновидность ИО
8. Информационные операции и атаки (обзор)
9. Информационные операции иностранных общественных и религиозных организаций (ИОРО)
10. Информационный терроризм
11. Информационная революция
12. Информация и человек
13. Информация и безопасность
14. Чувствительность и пороги безопасности при ИО
15. Конфликт и противоборство в контексте ИО
16. Информационное право и ИО
17. Информация и материя
18. Информационное общество
19. Информация и государство
20. Государственная система информационной безопасности
21. Информационное оружие как средство реализации ИО
22. Программно-математическое информационное оружие (ПМИО) как средство ИО
23. Интернет-зависимость
24. Средства противодействия программно-математическому оружию
25. Противодействие компьютерной преступности
26. Средства, атакующие каналы обмена
27. Программные закладки как средство кибератак
28. Компьютерные вирусы как средство кибератак
29. Компьютерные черви (КЧ) как средство кибератак
30. Компьютерные троянские кони (КТК) как средство кибератак

31. Компьютерные брандмауэры (КБ) как средство защиты от кибератак
32. Компьютерные демилитаризованные зоны (КДЗ) как средство защиты от кибератак
33. Компьютерные приманки и сигнализации (КП и КС) как средство защиты от кибератак
34. Компьютерные сканеры уязвимостей (КСУ) как средство защиты от кибератак
35. Частные виртуальные сети и кибератаки
36. Политические отношения в информационном обществе
37. Информационная борьба
38. Война и тайные информационные операции
39. Информационная война и право
40. Транснациональное информационное противоборство
41. Государственное регулирование в информационном противоборстве
42. Электронная цифровая подпись (ЭЦП) как средство защиты от кибератак
43. Компьютерная стеганография (КС) как средство защиты от кибератак
44. Человеческий фактор компьютерной безопасности (КБ)
45. Компьютерная разведка (КР) как компонент ИО
46. Оптическая разведка (ОР) как компонент ИО
47. Оптико-электронная разведка (ОЭР) как компонент ИО
48. Радиоэлектронная разведка (РЭР) как компонент ИО
49. Гидроакустическая и акустическая разведка (ГАР) как компонент ИО
50. Радиационная и химическая разведка (РХР) как компонент ИО
51. Сейсмическая и магнитометрическая разведка (СММР) как компонент ИО
52. Техническая разведка (ТР) как компонент ИО
53. Разведывательная система «Эшелон»
54. Аналитическая разведка как компонент ИО
55. Методология аналитической деятельности разведки
56. Аналитические технологии разведки
57. Психотронное оружие как средство ИО
58. Психотропное оружие (ПТО) как средство ИО
59. Программирование человека на основе концепции биокомпьютера как средство ИО
60. Концептуальное оружие (КО) как средство ИО
61. Биометрическая защита информации (БМЗИ) как средство защиты от кибератак
62. Криптография как средство защиты от кибератак (КТЗИ)
63. Квантовая криптография (КК) как средство защиты от кибератак (КТЗИ)

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

	В рамках изучения дисциплины предусмотрены следующие образовательные технологии:
5.1	**Информационные лекции**;
5.2	**практические занятия**: – Проведение после каждого раздела контрольных работ.
5.3	**самостоятельная работа студентов**: – изучение теоретического материала, – подготовка к лекциям и практическим занятиям, – работа с учебно-методической литературой, – оформление конспектов лекций, подготовка реферата, отчетов, – подготовка к текущему контролю успеваемости и к экзамену;
5.4	**консультации** по всем вопросам учебной программы.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6.1	**Контрольные вопросы и задания**
6.1.1	Используемые формы текущего контроля: – Рефераты; – Проверка домашних заданий.
6.1.2	Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения текущего контроля знаний.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1 Рекомендуемая литература

№ п/п	**Авторы, составители**	Заглавие	Годы издания. Вид издания	Обеспеченность
7.1.1. Основная литература				
7.1.1.1	Остапенко А.Г. М. Н. Иванкин	Обнаружение и нейтрализация вторжений в распределенных информационных системах [ЭЛ_РЕС] : Учеб. пособие / А. Г. Остапенко, М. Н. Иванкин. - Эл. текстовые, граф. дан. (366 Кб). - Воронеж : ФГБОУ ВПО "ВГТУ".	2013	1
7.1.2. Дополнительная литература				
7.1.2.1	Н. М. Радько, Ю. К. Язов	Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа [ЭЛ_РЕС] : Учеб. пособие / Н. М. Радько, Ю. К. Язов. - Эл. текстовые, граф. дан. (1,62 Мб). – Воронеж : ФГБОУ ВПО "ВГТУ".	2013	1
7.1.2.2	Н. М. Радько Ю. К. Язов	Проникновения в операционную среду компьютера: модели злоумышленного непосредственного доступа [ЭЛ_РЕС] : Учеб. пособие / Н. М. Радько, Ю. К. Язов. - Электрон. текстовые, граф. дан. (1,27 Мб). - Воронеж : ФГБОУ ВПО "ВГТУ".	2013	1

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	**Специализированная лекционная аудитория**, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой
8.2	**Дисплейный класс**, оснащенный компьютерными программами для проведения лабораторного практикума

ПРИЛОЖЕНИЕ 1

Карта обеспеченности рекомендуемой литературой

№ п/п	**Авторы, составители**	Заглавие	Годы издания. Вид издания	Обеспеченность
7.1.1. Основная литература				
Л1.1	Остапенко А.Г. М. Н. Иванкин	Обнаружение и нейтрализация вторжений в распределенных информационных системах [ЭЛ_РЕС] : Учеб. пособие / А. Г. Остапенко, М. Н. Иванкин. - Эл. текстовые, граф. дан. (366 Кб). - Воронеж : ФГБОУ ВПО "ВГТУ".	2013	1
7.1.2. Дополнительная литература				
Л2.1	Н. М. Радько, Ю. К. Язов	Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа [ЭЛ_РЕС] : Учеб. пособие / Н. М. Радько, Ю. К. Язов. - Эл. текстовые, граф. дан. (1,62 Мб). – Воронеж : ФГБОУ ВПО "ВГТУ".	2013	1
Л2.2	Н. М. Радько Ю. К. Язов	Проникновения в операционную среду компьютера: модели злоумышленного непосредственного доступа [ЭЛ_РЕС] : Учеб. пособие / Н. М. Радько, Ю. К. Язов. - Электрон. текстовые, граф. дан. (1,27 Мб). - Воронеж : ФГБОУ ВПО "ВГТУ".	2013	1

Зав. кафедрой _____ / А.Г. Остапенко /

Директор НТБ _____ / Т.И. Буковшина /

Утверждаю
зав. кафедрой СИБ
_____А. Г. Остапенко

Контрольно-измерительные материалы для проведения текущего и итогового контроля по дисциплине «Информационные операции и атаки в распределенных информационных системах»

Контрольно-измерительные материалы текущего контроля

Темы рефератов:

1. Информационные системы в социотехнических системах;
2. Технологии обработки информации в системах управления базами данных;
3. Сетевые технологии и системы распределенной обработки информации;
4. Информационные технологии в социотехнических системах;
5. Технологии разработки программ на основе алгоритмических и логических языков программирования;
6. Информационные технологии документационного обеспечения;
7. Технологии разработки программ на основе объектно-ориентированных языков программирования;
8. Технологии поддержки управленческих решений на основе систем искусственного интеллекта
9. Гипертекстовые технологии;
10. Технологии мультимедиа;
11. Технологии распознавания и синтеза речи;
12. Информационные технологии подготовки текстовых документов;
13. Технологии обеспечения информационной безопасности;
14. Технологии архивирования и сжатия данных;
15. Технические средства обеспечения информационных технологий;
16. Программные средства обеспечения информационных технологий;
17. Информационные технологии подготовки иллюстраций и презентаций на основе графических процессоров;
18. Системы обработки информации;
19. Тенденции развития современных информационных технологий;
20. Экспертные системы и системы поддержки принятия решений;
21. Системы интеллектуального проектирования.

Контрольно-измерительные материалы итогового контроля

Вопросы к экзамену 7 семестр:

1. Поясните отличия понятий множества и системы.
2. Обоснуйте мотивы формирования систем из множеств и наоборот.
3. Приведите базовые свойства системы.
4. Поясните сущность понятий угроза, уязвимость, ущерб и безопасность.
5. Поясните сущность информационно-кибернетических и информационно-психологических операций.
6. Перечислите основные виды информационных операций.
7. Приведите теоретико-множественную постановку задачи управления социотехническими системами.
8. Поясните сущность функций чувствительности в приложении к оценке безопасности социотехнических систем.
9. Приведите выражения для интегрального, усредненного, элементарного риска и защищенности социотехнических систем.
10. Поясните мотивы соперничества и сотрудничества социотехнических систем?
11. Перечислите качества информации, существенные для ее безопасности, а также операции, нарушающие безопасность.
12. Приведите структурную схему методики построения топологических моделей информационных операций.
13. Приведите классификацию сетевых угроз и атак.
14. На моделях поясните сущность атак, основанных на подборе имени пароля посредством перебора.
15. Приведите модели атак, основанных на анализе сетевого трафика.
16. На моделях поясните сущность атак, основанных на сканировании портов.
17. Приведите модели атак, основанных на внедрении ложного доверенного объекта.
18. На моделях поясните сущность атак, приводящих к отказу в обслуживании.
19. Поясните сущность интегрального усредненного риска и защищенности систем на примере различных законов дискретных распределений вероятностей успеха кибератаки.

Вопросы к зачету с оценкой 8 семестр:

1. Приведите модели простейших операций информационно-психологического управления.
2. Поясните сущность неформальных организаций.
3. Приведите специфику информационных технологий деструктивных культов.

4. Покажите особенности информационных операций, реализуемых в рамках политических технологий.

5. Перечислите средства противодействия деструктивным информационно-психологическим операциям.

6. Приведите стохастические модели информационно-управляющего воздействия.

7. Поясните стратегии информационно-управляющих воздействий.

8. На основе теории конфликтов проведите анализ мотивов террористической деятельности.

9. Поясните специфику информационных операций террористического характера.

10. На моделях покажите сущность процессов последействия информационных операций террористического характера.

11. Приведите сценарные модели информационных операций террористического характера.

12. Перечислите меры противодействия информационным операциям террористического характера.

13. Перечислите приемы кибертерроризма.

14. Опишите кризисный период, режим бифуркации и запас устойчивости социотехнических систем с учетом риска теракта.

15. Поясните качественно динамику информационного противоборства на основе поверхности риска теракта.

16. Обоснуйте сравнение теракта с детонатором информационной бомбы.