РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«Социотехнические основы информационной безопасности»

(наименование дисциплины (модуля) по УП)

Закреплена за кафедрой: систем информационной безопасности

Направление подготовки (специальности):
10.05.03 Информационная безопасность автоматизированных систем
(код, наименование)

Профиль: Обеспечение безопасности распределенных информационных систем

(название профиля по УП)

Часов по УП: 144**; Часов по РПД:** 144**;**
Часов по УП (без учета часов на экзамены): 144**; Часов по РПД:** 144**;**
Часов на интерактивные формы (ИФ) обучения по УП: 0**;**
Часов на интерактивные формы (ИФ) обучения по РПД: 0**;**
Часов на самостоятельную работу по УП: 36 (25%)**;**
Часов на самостоятельную работу по РПД: 36 (25%)**;**
Общая трудоемкость в ЗЕТ: 4**;**
Виды контроля в семестрах (на курсах): Зачеты с оценкой–1 и 2 семестр;
Курсовые работы - 1.
Форма обучения: очная**;**
Срок обучения: нормативный**.**

Распределение часов дисциплины по семестрам

Вид занятий	**№ семестров, число учебных недель в семестрах**																	
	1 / 20		2 / 22		3 / 18		4 / 18		5 / 18		6 / 18		7 / 18		8 / 10		Итого	
	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
Лекции	36	36	36	36													72	72
Лабораторные	0	0	0	0													0	0
Практические	0	0	0	0													0	0
Ауд. занятия	**36**	**36**	**36**	**36**													**72**	**72**
Сам. работа	**36**	**36**	**36**	**36**													**72**	**72**
Итого	**72**	**72**	**72**	**72**													**144**	**144**

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	**Цель изучения дисциплины** «Социотехнические основы обеспечения информационной безопасности» - обеспечить будущими инженерам, базовые знания и умения в области информационной безопасности для изучения последующих дисциплин**.**
1.2	**Для достижения цели ставятся задачи:**
1.2.1	системное знакомство с проблематикой обеспечения информационной безопасности;
1.2.2	освоение основ научно-методической, инженерно-технической и организационно-правовой составляющих данной отрасли человеческой деятельности
1.2.3	знакомство с ролью и местом кадрового обеспечения и специальностей высшего образования в области информационной безопасности, включая региональный аспект вышеперечисленных вопросов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООПВПО

Цикл (раздел) ООП: С1	код дисциплины в УП: С1.В.ДВ.1
2.1 Требования к предварительной подготовке обучающегося	
Для успешного освоения дисциплиныстудент должен иметь базовую школьную подготовку, иметь знания о сущности информационного пространства, его специфике и его составляющих (ИКП и ИПП), сущности и специфике информационных операций и атак в общем виде	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее	
С3.Б.8	Основы информационной безопасности
С3.Б.11	Технологическая защита информации
С3.Б.16	Управление информационной безопасности
С3.В.ОД.2	Социальные сети: риски и обеспечение безопасности
С3.В.ДВ.1.1	Управление рисками в распределенных информационных системах
С3.Б.19	Защита программ и данных
С3.Б.23	Методы анализа рисков

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОК-2	способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики.
ОК-3	способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач
ОК-4	способностью понимать движущие силы и закономерности исторического процесса, роль личности в истории, политической организации общества, способностью уважительно и бережно относиться к историческому наследию, толерантно воспринимать социальные и культурные различия
ОК-5	способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства.
ОК-9	способностью к логически-правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания.
ОК-10	способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой деятельности, развития социальных и профессиональных компетенций, изменения вида своей профессиональной деятельности.
ПК-5	способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.
ПК-6	способностью использовать нормативные правовые акты в своей профессиональной деятельности.
ПК-9	способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности.
ПК-33	способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	о разновидностях информационных угроз
3.1.2	о методах, средствах и системах обеспечения информационной безопасности
3.1.3	Государственный образовательный стандарт и учебный план своей специальности
3.1.4	объекты и виды профессиональной деятельности
3.2	**Уметь:**

3.2.1	формировать модели реализации угроз и процессы противодействия им
3.3	**Владеть:**
3.3.1	навыками противодействия угрозам информационной безопасности
3.3.3	системой знаний и понятии информация, безопасность, угроза, риск, шанс

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	Понятие «множества»	1	1-2	4				4
2	Понятие «система» и его применение в сфере информационной безопасности	1	3-4	4			4	8
3	Математическое описание «системы»	1	5-6	2			4	6
4	Методы представления систем	1	7-8	4			4	8
5	Критерии оценки систем	1	9-10	4			4	8
6	Анализ подходов к определению понятия «социотехническая система». Основы закономерности функционирования социотехнических систем	1	11-12	2			10	12
7	Понятие «риск» в контексте безопасности систем	1	13-14	4				4
8	Опасности социотехнических систем	1	15-16	2			6	8
9	Введение в конфликтологию. Формализация описания информационных конфликтов социотехнических систем	1	17-18	4				4
10	Стратегии и тактики информационных операций и атак, реализуемых в социотехнических системах	1	19-20	4			4	8
11	Рассмотрение террористической деятельности на основе теории конфликтов	2	1-2	4				4
12	Математические модели информационно-психологических процессов последствия теракта	2	3-4	4			8	12
13	Моделирование информационно-психологических операций	2	5-6	6			6	12
14	Доктрина информационной безопасности Российской Федерации	2	7-8	2				2
15	Угрозы информационной безопасности	2	9-10	2				2
16	Национальные интересы и их защита в информационной сфере	2	11-12	2			6	8

17	Безопасность национальных интересов в информационной сфере	2	13-14	2			8	10
18	Деятельность по обеспечению информационной безопасности	2	15-18	8			8	16
19	Органы государственной власти как субъекта обеспечения информационной безопасности	2	19-20	2				2
20	Подготовка специалистов в области информационной безопасности	2	21-22	4				4
Итого				72			72	144

4.1 Лекции

Неделя семестра	Тема и содержание лекции	Объем часов	В том числе, в интерактивной форме (ИФ)
1 семестр			
Понятие «множества»		**4**	
1-2	Теория множеств. Нечеткие множества. Операции над множествами. Индекс нечеткости.	4	
Понятие «система» и его применение в сфере информационной безопасности		**4**	
3-4	Понятие система, подсистема. Классификация систем. Цели системы. Структура системы. *Самостоятельное изучение*: Функции системы.	4	
Математическое описание «системы»		**2**	
5-6	Общие понятия теории систем. Абстрактные линейные системы. *Самостоятельное изучение*: Общие временные и динамические системы.	2	
Методы представления систем		4	
7-8	Классификация методов формализованного представления систем. Теоретико-множественный подход в описании систем. Условие обеспечения безопасности системы. *Самостоятельное изучение*: Применение графов для описания систем.	4	
Критерии оценки систем		**4**	
9-10	Эффективности систем. Виды критериев качества. Критерий пригодности. Критерий оптимальности. Критерий превосходства. *Самостоятельное изучение*: Помехоустойчивость.	4	
Анализ подходов к определению понятия «социотехническая система». Основы закономерности функционирования социотехнических систем		**2**	
11-12	Общесистемные закономерности в информационном аспекте функционирования социотехнических систем. Энтропийная компенсация, динамическое равновесие или баланс. Колебательные и циклические принципы функционирования. *Самостоятельное изучение*: Зависимость потенциала системы от структуры и характера взаимодействия ее элементов.Фоновая закономерность.	2	
Понятие «риск» в контексте безопасности систем		4	

13-14	Анализ информационных рисков. Оценка рисков. Понятие угроза. Определение уязвимости.	4	
Опасности социотехнических систем		2	
15-16	Опасности в информационно-психологическом пространстве. Опасности в информационно-кибернетическом пространстве. *Самостоятельное изучение*: Безопасность социотехнических систем.	2	
Введение в конфликтологию. Формализация описания информационных конфликтов социотехнических систем		4	
17-18	Понятие конфликт. Классификация конфликтов. Структурно-параметрическая модель конфликта.	4	
Стратегии и тактики информационных операций и атак, реализуемых в социотехнических системах		4	
19-20	Разновидности стратегий различных операций и атак. *Самостоятельное изучение*: Тактики реализации информационных операций и атак.	4	
Итого за 7 семестр		**36**	
2 семестр			
Рассмотрение террористической деятельности на основе теории конфликтов		**4**	
1-2	Специфика информационных операций террористического характера.	4	
Математические модели информационно-психологических процессов последствия теракта		**4**	
3-4	Общая модель эффекта последствия теракта. Механизмы реализации информационно-управляющего воздействия в период последствии теракта. *Самостоятельное изучение*: Риск-анализ информационно-управляющих в период последствий теракта	4	
Моделированиеинформационно-психологических операций		**6**	
5-6	Разновидность моделей. Классификация модельных представлений. *Самостоятельное изучение*: Классификация угроз информационно-психологической безопасности региона.	6	
Доктрина информационной безопасности Российской Федерации		2	
7-8	Основные источники угроз информационной безопасности РФ. Методы обеспечения информационной безопасности РФ.	2	
Угрозы информационной безопасности		**2**	
9-10	Угрозы национальным интересам в информационной сфере.	2	
Национальные интересы и их защита в информационной сфере		**2**	
11-12	Национальные интересы и их содержание. *Самостоятельное изучение*: Национальные интересы в информационной сфере	2	
Безопасность национальных интересов в информационной сфере		2	
13-14	Информация, информационная инфраструктура и правовой статус человека и гражданина в области информационной деятельности. *Самостоятельное изучение*: Деятельность субъектов национальных интересов.	2	
Деятельность по обеспечению информационной безопасности		8	
15-18	Цель деятельности по обеспечению информационной безопасности. Принципы и формы деятельности. Методы деятельности по обеспечению информационной безопасности. *Самостоятельное изучение*: Средства обеспечения информационной безопасности.	8	
Органы государственной власти как субъекта обеспечения		2	

информационной безопасности			
19-20	Органы государственной власти как субъекта обеспечения информационной безопасности	2	
Подготовка специалистов в области информационной безопасности		4	
21-22	Подготовка специалистов в области информационной безопасности	4	
Итого за 8 семестр		**36**	
Всего		**72**	

4.2 Практические занятия.

Не предусмотрены.

4.3 Лабораторные работы.

Не предусмотрены.

4.4 Самостоятельные работы студента.

Неделя семестра	Содержание СРС	Виды контроля	Объем часов
1 семестр		**Зачет**	**36**
4	Функции системы.	проверка домашнего задания	4
6	Общие временные и динамические системы.	проверка домашнего задания	4
8	Применение графов для описания систем	проверка домашнего задания	4
10	Помехоустойчивость.	проверка домашнего задания	4
11	Зависимость потенциала системы от структуры и характера взаимодействия ее элементов	проверка домашнего задания	6
12	Фоновая закономерность.	проверка домашнего задания	4
16	Безопасность социотехнических систем	проверка домашнего задания	6
20	Тактики реализации информационных операций и атак.	проверка домашнего задания	4
2 семестр		**Зачет**	**36**
4	Риск-анализ информационно-управляющих в период последствий теракта	проверка домашнего задания	8
6	Классификация угроз информационно-психологической безопасности региона.	проверка домашнего задания	6
12	Национальные интересы в информационной сфере	проверка домашнего задания	6
14	Деятельность субъектов национальных интересов.	проверка домашнего задания	8
18	Средства обеспечения информационной безопасности.	проверка домашнего задания	8

4.5 Темы курсовых работ.

1. Анализ Client-IRC.
2. Анализ Client-P2P.
3. Анализ Client-SMTP.
4. Анализ Dialer.
5. Анализ Downloader.
6. Анализ FraudTool.
7. Анализ вредоносных программ типа Backdoor.
8. Анализ NetTool.
9. Анализ RemoteAdmin.
10. Анализ Dialer.
11. Анализ RiskTool.
12. Анализ Server-Web.
13. Анализ Server-Proxy.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

	В рамках изучения дисциплины предусмотрены следующие образовательные технологии:
5.1	**Информационные лекции**;
5.2	**Практические занятия**: – работа в команде - совместное обсуждение вопросов лекций, домашних заданий, решение творческих задач; – выступления по темам рефератов, – проведение расчетных 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: – Контрольные вопросы; – 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, Г.А.	Информационные операции и атаки в социотехнических системах : учеб. пособие. – М. : Горячая линия –Телеком, 2007. – 134 с. : ил. – ISBN 5-93517-288-7 : 121-00. Рекомендовано в качестве учеб. пособия УМО по образованию в области информационной безопасноти для студентов	2007-печат.	1
7.1.1.2	Остапенко Г.А.	Информационные операции [Электронный ресурс] : учеб. пособие. – Электрон. дан. (1 файл :3045 Кбайта). – Воронеж : ГОУВПО «Воронежский государственный технический университет», 2006. – 1 CD-ROM. – 30-00. Допущено УМО по образованию в области информационной безопасности для студентов вузов	2006 Электр.	1,0
7.1.1.3	Дуров В.П.	Моделирование риск-анализа социотехнических систем [Электронный ресурс] : учеб. пособие. – Электрон. текстовые дан. (3087 Кб). – Воронеж : ГОУВПО «Воронежский государственный технический университет», 2007. – 1 CD-ROM. – 30-00.	2007-электр.	1,0
7.1.1.4	О.А. Кадомская , А.Ф. Мешкова.	Средства поддержки принятия решений по защите информации в органах государственной власти. Учеб. пособие. Воронеж: Воронеж. гос. техн. ун-т, 2008.- 427 с	2008-электр.	1,0
7.1.1.5	Остапенко А.Г., Плотников Д.Г., Машин С.В.	Методология риск-анализа и моделирование кибернетических систем, атакуемых вредоносным программным обеспечением	2012-электр.	1,0
7.1.2. Дополнительная литература				
7.1.2.1	Остапенко О.А., Батищев Р.В.	Опасность, ущербы и риски систем: учеб. пособие / О.А. Остапенко, Р.В. Батищев – Воронеж: НОУВПО «Международный институт компьютерных технологий», 2007. - 206 с.	2007-печат.	0,2
7.1.3 Методические разработки				
7.1.3.1	А.Г. Остапенко	Рабочая программа по дисциплине «Введение в специальность»	2005 электр.	1
7.1.3.2	Г.А. Остапенко В.Г. Дуров О.А. Остапенко	Методические указания к выполнению индивидуальных заданий по дисциплине «Введение в специальность»	2005 электр.	1
7.1.3.3	А.Г. остапенко	Рабочая программа по дисциплине «Введение в специальность»	2005 электр.	1
7.1.1.4	А.Г. Остапенко	Рабочая программа по дисциплине «Введение в	2005	1

		специальность»	электр.	
7.1.4 Программное обеспечение и интернет ресурсы				
7.1.4.1	Методические указания к выполнению лабораторных работ **представлены насайте: http://vorstu.ru/kafedrry/ftf/kaf/frp/uchpl/**			

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

ПРИЛОЖЕНИЕ 1

Карта обеспеченности рекомендуемой литературой

№ п/п	Авторы, составители	Заглавие	Год издания. Вид издания.	Обеспеченность
1. Основная литература				
Л1.1	Остапенко, Г.А.	Информационные операции и атаки в социотехнических системах : учеб. пособие. – М. : Горячая линия –Телеком, 2007. – 134 с. : ил. – ISBN 5-93517-288-7 : 121-00. Рекомендовано в качестве учеб. пособия УМО по образованию в области информационной безопасноти для студентов	2007-печат.	1
Л1.2	Остапенко Г.А.	Информационные операции [Электронный ресурс] : учеб. пособие. – Электрон. дан. (1 файл :3045 Кбайта). – Воронеж : ГОУВПО «Воронежский государственный технический университет», 2006. – 1 CD-ROM. – 30-00. Допущено УМО по образованию в области информационной безопасности для студентов вузов	2006 Электр.	1,0
Л1.3	Дуров В.П.	Моделирование риск-анализа социотехнических систем [Электронный ресурс] : учеб. пособие. – Электрон. текстовые дан. (3087 Кб). – Воронеж : ГОУВПО «Воронежский государственный технический университет», 2007. – 1 CD-ROM. – 30-00.	2007-электр.	1,0
Л1.4	О.А. Кадомская , А.Ф. Мешкова.	Средства поддержки принятия решений по защите информации в органах государственной власти. Учеб. пособие. Воронеж: Воронеж. гос. техн. ун-т, 2008.- 427 с	2008-электр.	1,0
Л1.5	Остапенко А.Г., Плотников Д.Г., Машин С.В.	Методология риск-анализа и моделирование кибернетических систем, атакуемых вредоносным программным обеспечением	2012-электр.	1,0
2. Дополнительная литература				
Л2.1	Остапенко О.А., Батищев Р.В.	Опасность, ущербы и риски систем: учеб. пособие / О.А. Остапенко, Р.В. Батищев – Воронеж: НОУВПО «Международный институт компьютерных технологий», 2007. - 206 с.	2007-печат.	0,2
3. Методические разработки				

Л3.1	А.Г. Остапенко	Рабочая программа по дисциплине «Введение в специальность»	2005 электр.	1
Л3.2	Г.А. Остапенко В.Г. Дуров О.А. Остапенко	Методические указания к выполнению индивидуальных заданий по дисциплине «Введение в специальность»	2005 электр.	1
Л3.3	А.Г. остапенко	Рабочая программа по дисциплине «Введение в специальность»	2005 электр.	1
Л3.4	А.Г. Остапенко	Рабочая программа по дисциплине «Введение в специальность»	2005 электр.	1

Зав. кафедрой СИБ _____ /А.Г. Остапенко /

Директор НТБ _____ / /

Контрольно-измерительные материалы для проведения текущего контроля и промежуточной и итоговой аттестации по дисциплине «Социотехнические основы информационной безопасности»

Контрольно-измерительные материалы итогового контроля

Вопросы к зачету с оценкой 1-й семестр:

1. Теория множеств.
2. Нечеткие множества.
3. Операции над множествами.
4. Индекс нечеткости.
5. Понятие система, подсистема.
6. Классификация систем.
7. Цели системы.
8. Структура системы.
9. Функции системы.
10. Общие понятия теории систем.
11. Абстрактные линейные системы.
12. Общие временные и динамические системы.
13. Классификация методов формализованного представления систем.
14. Теоретико-множественный подход в описании систем.
15. Условие обеспечения безопасности системы.
16. Применение графов для описания систем.
17. Эффективности систем.
18. Виды критериев качества.
19. Критерий пригодности.
20. Критерий оптимальности.
21. Критерий превосходства.
22. Помехоустойчивость.
23. Общесистемные закономерности в информационном аспекте функционирования социотехнических систем.
24. Энтропийная компенсация, динамическое равновесие или баланс.
25. Колебательные и циклические принципы функционирования.
26. Зависимость потенциала системы от структуры и характера взаимодействия ее элементов.
27. Фоновая закономерность.
28. Анализ информационных рисков.
29. Оценка рисков.
30. Понятие угроза.
31. Определение уязвимости.

32. Опасности в информационно-психологическом пространстве.
33. Опасности в информационно-кибернетическом пространстве.
34. Безопасность социотехнических систем.
35. Понятие конфликт.
36. Классификация конфликтов.
37. Структурно-параметрическая модель конфликта.
38. Разновидности стратегий различных операций и атак.
39. Тактики реализации информационных операций и атак.

Контрольно-измерительные материалы итогового контроля

Вопросы к зачету с оценкой 2-й семестр:

1. Специфика информационных операций террористического характера.
2. Общая модель эффекта последствия теракта.
3. Механизмы реализации информационно-управляющего воздействия в период последствии теракта.
4. Риск-анализ информационно-управляющих в период последствий теракта.
5. Разновидность моделей информационно-психологических операций.
6. Классификация модельных представлений.
7. Классификация угроз информационно-психологической безопасности региона.
8. Основные источники угроз информационной безопасности РФ.
9. Методы обеспечения информационной безопасности РФ.
10. Угрозы национальным интересам в информационной сфере.
11. Национальные интересы и их содержание.
12. Национальные интересы в информационной сфере.
13. Информация, информационная инфраструктура и правовой статус человека и гражданина в области информационной деятельности.
14. Деятельность субъектов национальных интересов.
15. Цель деятельности по обеспечению информационной безопасности.
16. Принципы и формы деятельности.
17. Методы деятельности по обеспечению информационной безопасности.
18. Средства обеспечения информационной безопасности.
19. Органы государственной власти как субъекта обеспечения информационной безопасности