РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Социальные сети: риски и обеспечение 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 информационнной безопасности распределённых информационных систем" "

(название профиля по УП)

Часов по УП: 468; **Часов по РПД:** 468;

Часов по УП (без учета часов на экзамены): 468; **Часов по РПД:** 468;

Часов на самостоятельную работу по УП: 172 (%);

Часов на самостоятельную работу по РПД: 172 (%);

Общая трудоемкость в ЗЕТ: 13**;**

Виды контроля в семестрах (на курсах): Экзамены - 1; Зачеты - 0; Зачеты с оценкой – 2; Курсовые проекты - 1; Курсовые работы - 0.

Форма обучения: очная**;**

Срок обучения: нормативный**.**

Распределение часов дисциплины по семестрам

Вид занятий	**№ семестров, число учебных недель в семестрах**																							
	1 / 18		2 / 20		3 / 18		4 / 20		5 / 18		6 / 20		7 / 18		8 / 20		9 / 18		10 / 20		11 / 18		Итого	
	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
Лекции													54	54	40	40	36	36					130	130
Лабораторные													0	0	0	0							0	0
Практические													54	54	40	40	36	36					130	130
Ауд. занятия													**108**	**108**	**80**	**80**	**72**	**72**					**260**	**260**
Сам. работа													**72**	**72**	**36**	**36**	**64**	**64**					**172**	**172**
Итого													**180**		**116**		**172**						**468**	

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Основная цель изучения данной дисциплины заключается в ознакомлении с проблемой социальных сетей с точки зрения повышения защищённости пользователей путём анализа моделей распространения вредоносного программного обеспечения, а также с помощью построения риск-моделей информационно-психологического воздействия на пользователей социальных сетей.
1.2	**Для достижения цели ставятся задачи:**
1.2.1	− способность управлять информационными рисками;
1.2.2	− прогнозировать эффективность защиты распределенных информационных систем, подвергающихся деструктивному воздействию;

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Цикл (раздел) ООП: С3.	код дисциплины в УП: С3.В.ОД2.
2.1 Требования к предварительной подготовке обучающегося	
Требования к знаниям: - разновидности информационных операций и атак, реализуемых в СТИС, способы их реализации в информационном пространстве; - способы и приемы террористических и деструктивных воздействий на информационные системы; основы построения антитеррористических информационно-аналитических систем; - основы построения моделей для защиты от террористических и деструктивных воздействий; - уязвимые места информационных систем, чаще всего подвергающиеся атакам;	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее	
С2.Б4.	Теория вероятностей и математическая статистика
С2.В.ДВ.1	Математическое моделирование ИОА
С2.В2.ДВ.1	Математические модели информационного противоборства
С2.Б2.	Математический анализ
С2.Б.5.	Математическая логика и теория алгоритмов
С3.Б.18	Информационная безопасность распределенных информационных систем

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-4	способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности;
ПК-13	способностью проводить математическое моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований;
ПК-14	способностью выявлять тенденции развития информационной безопасности телекоммуникационных систем;
ПСК-7.2	способностью разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	- основные уязвимости социальных сетей для атак вредоносного ПО и информационно-психологического воздействия на пользователей;
3.1.2	- опасные и вредоносные факторы воздействия на элементы социальных сетей и пользователей;
3.1.3	- основные виды ущерба при реализации атак и воздействии на пользователей социальных сетей;
3.2	**Уметь:**
3.2.1	- применять основные меры и средства защиты социальных сетей от атак вредоносного ПО и воздействия на пользователей
3.2.2	- оценивать вероятностные и временные характеристики реализации атак вредоносного ПО и воздействия на пользователей социальных сетей
3.3	**Владеть:**
3.3.1	- навыками построения математических моделей осуществления атак на социальных сетей и воздействий на пользователей
3.3.2	- методикой анализа рисков при реализации атак вредоносного ПО и воздействий на пользователей социальных сетей

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ П./п	Наименование раздела дисциплины	Семестр	Неделя семестра	Вид учебной нагрузки и их трудоемкость в часах			
				Лекции	Практические занятия	СРС	Всего часов
1	Введение в теорию социальных сетей	7	1-3	10	10	14	34
2	Методы анализа компьютерных социальных сетей	7	4-6	12	12	16	40
3	Основные направления исследования компьютерных социальных сетей	7	7-8	10	10	14	34

4	Параметры сложных сетей	7	9-15	10	10	12	32
5	Модели анализа социальных сетей	7	16-18	12	12	16	40
6	Программные приложения для анализа социальных сетей	8	1-4	6	6	6	18
7	Модели формирования и роста сетей	8	5-7	8	8	4	20
8	Анализ структуры связей и роли узлов	8	8-11	6	6	6	18
9	Метрики структурной эквивалентности узлов.	8	12-15	6	6	6	18
10	Сетевые сообщества	8	16-17	4	4	8	16
11	Диффузия и распространение эпидемий.	8	17-18	6	6	4	16
12	Модели распространение влияния	8	19-20	4	4	2	10
13	Модели достижения консенсуса	9	1-3	8	8	12	28
14	Информационные каскады	9	4-6	6	6	12	24
15	Модель пространственной сегрегации	9	7-8	6	6	12	24
16	Информационные риски и эпистойкость безмасштабных сетей	9	9-15	8	8	14	30
17	Подходы к управлению эпистойкостью атакуемой безмасштабной сети	9	16-18	8	8	14	30
Итого				130	130	172	

4.1 Лекции

Неделя семестра	Тема и содержание лекции	Объем часов
	7 семестр	**54**
1-3	Введение в теорию социальных сетей. Основные понятия в теории сетей. Основные измеряемые свойства сетей. Примеры сетей. История исследования социальных сетей	10
4-6	Методы анализа компьютерных социальных сетей. Степенное распределение. Масштабно-инвариантные сети (scale-free networks). Распределение Парето, нормализация, моменты. Закон Ципфа. Граф ранк-частота. Методы измерений параметров сетей.	12
7-8	Основные направления исследования компьютерных социальных сетей	10
9-15	Параметры сложных сетей. Параметры узлов сети. Общие параметры сети. Распределение степеней узлов. Путь между узламию Коэффициент кластерности. Посредничество. Эластичность сети. Структура сообщества.	10
16-18	Модели анализа социальных сетей. Модель «слабых связей». Модель Уаттса-Строгатца. Графовые модели. Стохастические блоковые модели. Вероятностные графовые модели. Анализ центральности и других локальных свойств	12
	8 семестр	**40**
1-4	Программные приложения для анализа социальных сетей	6
5-7	Модели формирования и роста сетей	8
8-11	Анализ структуры связей и роли узлов. Понятия центральности и	6

	престижа. Модельные графы. Degree centrality, closeness centrality, betweenness centrality, статус/rank prestige (eigenvector centrality). Центральность сети. Анализ связей. Алгоритм PageRank. Стохастические матрицы. Теорема Perrona-Frobenius. Степенные итерации. Нахождение собственного вектора. Hubs и Authorities.	
12-15	Метрики структурной эквивалентности узлов. Эвклидово расстояние. Расстояние Хэмминга. Корреляционный коэффициент. Сходство по косинусу). Ассортативное смешивание Модулярность Ассортативный коэффициент. Смешивание по степеням узлов .	6
16-17	Сетевые сообщества. Понятие сетевых сообществ (network communities). Плотность связей. Метрики. Разделение графа на части (graph partitioning). Разрезы (cuts) в графе. Min-cut, quotent and normalized cuts метрики. Divisive and agglomerative algorithms. Repeated bisection. Корреляционная матрица. Классификация алгоритмов нахождения сообществ. Edge Betweenness. Newman-Girvin.	4
17-18	Уравнение диффузии. Диффузия на сетях. Дискретный оператор Лапласа, Матрица Лапласа, решение уравнения диффузии на графе. Случайные блуждания на графе. Модели SI, SIR, SIS. Решения дифференциальных уравнений. Предельные случаи.	6
19-20	Модели распространение влияния. Пороговые модели принятия решений. Granovetter's Threshold model коллективного поведения. Определение наиболее влиятельных узлов.	4
	9 семестр	**36**
1-3	Модели достижения консенсуса. Обучение в сети. Понятие консенсуса в сети. Модель De Groot. Условия достижимости консенсуса.	8
4-6	Информационные каскады. Observational learning. Модели каскадов. Условия возникновения информационных каскадов. Модели каскадов	6
7-8	Модель пространственной сегрегации. Модель сегрегации Шеллинга.	6
9-15	Информационные риски и эпистойкость безмасштабных сетей	8
16-18	Подходы к управлению эпистойкостью атакуемой безмасштабной сети	8
Итого часов		**130**

4.2 Практические занятия.

Неделя семестра	Тема и содержание практических занятий	Объем часов	Вид контроля
	7 семестр	**54**	
1-3	Решения задачи построения эквивалентного графа	4	Лабораторная работа
4-6	Построить распределение степеней узлов в фрагменте “internet routing system”. (http://www.routeviews.org/). Показать, что	4	Практическая работа за компьютерами

	распределение носит степенной характер. Оценить значение показателя степени по наклону кривой. Построить кумулятивную функцию распределения, найти значение показателя степени по наклону кривой. Вычислить показатель степени используя метод максимального правдоподобия. Сравнить полученные результаты		
7-8	Вычислить корреляционную матрицу (Pearson correlation) структурной эквивалентности узлов в сетях “karate_club” и “dolphins” и визуализировать ее командой pcolor. 2) Вычислить величину ассортативного смешивания по степеням узлов (assortativity coefficient) в сетях “Princeton”, “Georgetown”, “internet autonomous”, “political blogs”.	4	Практическая работа за компьютерами
9-15	Модели анализа социальных сетей	6	Рефераты
16-18	Закон Ципфа	8	Рефераты
	8 семестр	**40**	
1-4	Нахождение структуры в графах. Graph motiffs, k-cores, diad and triad census	6	Рефераты
5-7	Модели SI, SIR, SIS на сетях. Приближенные решения дифференциальных уравнений на сетях. Предельные случаи. Иммунизация.	4	Рефераты
8-11	Имплементировать SIS/SIR модели распространения эпидемии в сетях. Исследовать поведение моделей на следующих сетях: 1) регулярная двумерная решетка 2) двумерная модель малого мира 3) случайный граф 4) модель предпочтительного присоединения BA 5) данная сеть. Для каждой модели/сети построить усредненную зависимость распространения инфекции (% зараженных узлов) от времени при фиксированном выборе параметров модели.	4	Практическая работа за компьютерами
12-15	Визуализировать социальные сети, полученными с различных источников, в том числе и взятых непосредственно с социальных медиа сайтов таких, как Facebook и Twitter и др.	6	Практическая работа за компьютерами
16-17	Провести анализ дружеских связей VK, Facebook, Twitter и д.р. для личной странички с помощью Wolfram Mathematica и визуализировать их.	4	Практическая работа за компьютерами
17-18	Алгоритм HITS. Сравнение ранжировок. Расстояние Kendall-Tau.	4	Рефераты
19-20	Спектральные методы. Максимизация	4	Рефераты

	модулярности (Newman) Аппроксимационные алгоритмы. Randomized min-cut (Karges's algorithm). Multilevel алгоритмы. Metis алгоритм. Локальная кластеризация. Conductance. Алгоритм Nibble.		
	9 семестр	**36**	
1-3	Обнаружить и визуализировать сообщества такие, как семья, коллеги по работе, школьные друзья в сети друзей в Facebook и других социальных сетях		Практическая работа за компьютерами
4-6	Вычислить центральность, престиж, гемофильность и ассортативное группирование визуализированных сообществ.		Практическая работа за компьютерами
7-8	Используя возможностей системы Mathematica по теории вероятностей и статистике для анализа социальной сети и найти основные статистических величин и провести анализ распределения степеней входящих рёбер		Практическая работа за компьютерами
9-15	Найти и визуализировать коэффициент глобальной кластеризации случайного графа. Создать тепловую карту полученных графов по значениям коэффициентов		Практическая работа за компьютерами
16-18	Сегрегация на сетях. Условия возникновения сеграгации.		Рефераты
Итого часов		**130**	

4.3. Самостоятельная работа студента (СРС).

Неделя семестра	Содержание СРС	Вид контроля	Объем часов
	7 семестр		**72**
1-3	Моделис порогами	**Реферат**	14
4-6	Модели с порогами	**Реферат**	16
7-8	Модели независимых каскадов	**Реферат**	14
9-15	Модели просачивания и заражения	**Реферат**	12
16-18	Модели Изинга	**Реферат**	16
	8 семестр		36
1-4	Модели на основе клеточных автоматов	**Реферат**	6
5-7	Модели на основе цепей Маркова	**Реферат**	4
8-11	Модели взаимной информированности	**Реферат**	6
12-15	Модели согласованных коллективных действий	**Реферат**	6
16-17	Модели коммуникаций	**Реферат**	8
17-18	Модели стабильности сети	**Реферат**	4

19-20	Модели информационного влияния и управления	**Реферат**	2
	9 семестр		64
1-3	Модели информационного противоборства	**Реферат**	12
4-6	Векторно-пространственная модель поиска	**Реферат**	12
7-8	Информационные операции как социальные процедуры	**Реферат**	12
9-15	Моделирование деструктивного воздействия на сети	**Реферат**	14
16-18	Теория перколяции и моделирование атак на сети	**Реферат**	14
Итого часов			**172**

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 самостоятельно по учебнику. • Подготовка к практическим занятиям. • Подготовка к курсовому проектированию.
5.4	**Консультации по всем вопросам учебной программы**

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ 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 работы; • Проверка домашних заданий;
6.1.2	Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения аттестации. Фонд включает вопросы к экзамену и зачету
6.2	**Темы письменных работ**
6.2.1	Контрольная работа по теме «Введение в теорию социальных сетей»
6.2.2	Контрольная работа по теме «Методы анализа компьютерных социальных сетей»
6.2.3	Контрольная работа по теме «Основные направления исследования компьютерных социальных сетей»
6.2.4	Контрольная работа по теме «Параметры сложных сетей»
6.2.5	Контрольная работа по теме «Модели анализа социальных сетей»
6.2.6	Контрольная работа по теме «Программные приложения для анализа социальных сетей»

6.2.7	Контрольная работа по теме «Модели формирования и роста сетей»
6.2.8	Контрольная работа по теме «Анализ структуры связей и роли узлов»
6.2.9	Контрольная работа по теме «Метрики структурной эквивалентности узлов»
6.2.10	Контрольная работа по теме «Сетевые сообщества»
6.2.11	Контрольная работа по теме «Диффузия и распространение эпидемий»
6.2.12	Контрольная работа по теме «Модели распространение влияния»
6.2.13	Контрольная работа по теме «Модели достижения консенсуса»
6.2.14	Контрольная работа по теме «Информационные каскады»
6.2.15	Контрольная работа по теме «Модель пространственной сегрегации»
6.2.16	Контрольная работа по теме «Информационные риски и эпистойкость безмасштабных сетей»
6.2.17	Контрольная работа по теме «Подходы к управлению эпистойкостью атакуемой безмасштабной сети»
6.3	**Другие виды контроля**
6.3.1	Контроль за выполнение курсового проекта в соответствии с установленным графиком его выполнения. Темы курсовых работ: - Выполнить программную реализацию инструмента для выполнения анализа эффективности применения комплексов мер противодействия угрозам воздействия вредоносного ПО и информационно-психологического воздействия на пользователей социальных сетей. - Реализации возможности построения социальных графов пользователей других онлайн-социальных сетей; - Разработка функционала для выявления и анализа кластеров социального графа;

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. Н. М. Радько, А. Ф. Мешкова	Нейронные модели обнаружения вторжений и атак на компьютерные сети [ЭЛ/РЕС] : учеб. пособие / Г. А. Остапенко, Н. М. Радько, А. Ф. Мешкова. - Электрон. дан. (1 файл : 2402Кб). - Воронеж : ГОУВПО "ВГТУ", 2007. - 1 файл. - 30-00.	2007	1
7.1.1.2	Щербаков В.Б. Н. Н. Толстых, Г. А. Остапенко	Обнаружение вторжений на основе анализа фрагментов унитарного кода [ЭЛ/РЕС] : учеб. пособие / В. Б. Щербаков, Н. Н. Толстых, Г. А. Остапенко. - Электрон. дан. (1 файл : 1454 Кб). - Воронеж : ГОУВПО "ВГТУ", 2007. - 1 файл. - 30-00.	2007	1
7.1.1.	Г. А. Остапенко	Методическое обеспечение оценки	2011	24

3	Менжулин Р.В.; Коваленко Д.М.; Машин С.В.; Жуков М.М.; Лыков С.В.; Плотников Д.Г.; Куликов С.С.	и регулирования рисков распределенных информационных систем : Учеб. пособие / Г. А. Остапенко [и др.]. - Воронеж : ФГБОУ ВПО "ВГТУ", 2011. - 178 с. - 182-77;		
7.1.1.4	Остапенко А.Г. Д. Г. Плотников, С. В. Машин.	Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обес-печением [ЭЛ/РЕС] : Учеб. пособие / А. Г. Остапенко, Д. Г. Плотников, С. В. Машин. - Эл. текстовые, граф. дан. (112 Кб). - Воронеж : ФГБОУ ВПО "ВГТУ", 2012. - 1 файл. - 30-00.	2012	1
7.1.2. Дополнительная литература				
7.1.2.1	Г.А. Остапенко, А. Е. Дешина.	Компьютерные преступления [ЭЛ/РЕС] : Учеб. пособие / Г. А. Остапенко, А. Е. Дешина. - Электрон. текстовые, граф. дан. (1,37 Мб). - Воронеж : ФГБОУ ВПО "ВГТУ", 2013. - 1 файл.	2013	1
7.1.2.2	В. Б. Щербаков	Обнаружение сетевых вторжений [ЭЛ/РЕС] : Учеб. пособие / В. Б. Щербаков. - Электрон. текстовые, граф. дан. (423 Кб). - Воронеж : ФГБОУ ВПО "ВГТУ", 2013. - 1 файл. - 30-00.	2013	1
7.1.2.3		Модели обнаружения сетевых вторжений [ЭЛ/РЕС] : Учеб. пособие. - Электрон. текстовые, граф. дан. (652 Кб). - Воронеж : ФГБОУ ВПО "ВГТУ", 2013. - 1 файл. - 30-00.	2013	1
7.1.2.4	Кулаков В.Г.; Соловьев А.К.; Кобяшов В.Г.	Компьютерные преступления в сфере государственного и муниципального управления / под. ред. А. Г. Остапенко. - Воронеж : ВИ МВД России, 2002. - 116 с. - ISBN 5-88591-002-4 : 20.00.	2002	50
7.1.2.5		Моделирование информационных операций и атак в сфере государственного и муниципального управления : Монография / под ред. В.И.Борисова. - Воронеж : ВИ МВД России, 2004. - 144 с. - Дар кафедры СИБ. - 100-00.	2004	25

7.1.2.6	Кулаков В.Г.; Кобяшев А.Б.; Андреев А.Б.; Линец А.Л.; Дидюк Ю.Е.; Макаров О.Ю.	Оптимальный синтез и анализ эффективности комплексов защиты информации : Монография. - Воронеж : ВГТУ, 2006. - 137 с. - 30-00.	2006	25
7.1.2.7	Дуров В.П.	Программно-аппаратная защита информации [Электронный ресурс] : учеб. пособие. - Электрон. дан. (1 файл :6681088 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.	2006	1
7.1.2.8	Остапенко Г.А.	Логико-лингвистические модели атак на компьютерные системы [Электронный ресурс] : Учеб. пособие / под ред. А. Г. Остапенко. - Электрон. текстовые, граф. дан. (8452435 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.	2008	1
7.1.2.9	Пархоменко А.П. Мешкова А.Ф.; Менжулин Р.В.	Основные проблемы и особенности защиты информации в банковских системах: модели нарушителей [Электронный ресурс] / под ред. Г. С. Остапенко. - Электрон. текстовые, граф. дан. (1245435 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.	2008	1

ПРИЛОЖЕНИЕ 3

Карта обеспеченности рекомендуемой литературой

№ п/п	**Авторы, составители**	**Заглавие**	**Год издания. Вид издания.**	**Обеспеченность**
1. Основная литература				
Л1.1	Остапенко, Г.А. Н. М. Радько, А. Ф. Мешкова	Нейронные модели обнаружения вторжений и атак на компьютерные сети [ЭЛ/РЕС] : учеб. пособие / Г. А. Остапенко, Н. М. Радько, А. Ф. Мешкова. - Электрон. дан. (1 файл : 2402Кб). - Воронеж : ГОУВПО "ВГТУ", 2007. - 1 файл. - 30-00.	2007	1
Л1.2	Щербаков В.Б. Н. Н. Толстых,	Обнаружение вторжений на основе анализа фрагментов унитарного кода [ЭЛ/РЕС] : учеб.	2007	1

	Г. А. Остапенко	пособие / В. Б. Щербаков, Н. Н. Толстых, Г. А. Остапенко. - Электрон. дан. (1 файл : 1454 Кб). - Воронеж : ГОУВПО "ВГТУ", 2007. - 1 файл. - 30-00.		
Л1.3	Г. А. Остапенко МенжулинР.В. КоваленкоД.М. МашинС.В. Жуков М.М. Лыков С.В. ПлотниковД.Г. Куликов С.С.	Методическое обеспечение оценки и регулирования рисков распределенных информационных систем : Учеб. пособие / Г. А. Остапенко [и др.]. - Воронеж : ФГБОУ ВПО "ВГТУ", 2011. - 178 с. - 182-77;	2011	24
Л1.4	ОстапенкоА.Г. Д. Г.Плотников, С. В. Машин.	Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обес-печением [ЭЛ/РЕС] : Учеб. пособие / А. Г. Остапенко, Д. Г. Плотников, С. В. Машин. - Эл. текстовые, граф. дан. (112 Кб). - Воронеж : ФГБОУ ВПО "ВГТУ", 2012. - 1 файл. - 30-00.	2012	1
2.Дополнительная литература				
Л2.1	Г.А. Остапенко, А. Е. Дешина.	Компьютерные преступления [ЭЛ/РЕС] : Учеб. пособие / Г. А. Остапенко, А. Е. Дешина. - Электрон. текстовые, граф. дан. (1,37 Мб). - Воронеж : ФГБОУ ВПО "ВГТУ", 2013. - 1 файл.	2013	1
Л2.2	В. Б. Щербаков	Обнаружение сетевых вторжений [ЭЛ/РЕС] : Учеб. пособие / В. Б. Щербаков. - Электрон. текстовые, граф. дан. (423 Кб). - Воронеж : ФГБОУ ВПО "ВГТУ", 2013. - 1 файл. - 30-00.	2013	1
Л2.3		Модели обнаружения сетевых вторжений [ЭЛ/РЕС] : Учеб. пособие. - Электрон. текстовые, граф. дан. (652 Кб). - Воронеж : ФГБОУ ВПО "ВГТУ", 2013. - 1 файл. - 30-00.	2013	1
Л2.4	Кулаков В.Г.; Соловьев А.К.; Кобяшов В.Г.	Компьютерные преступления в сфере государственного и муниципального управления / под. ред. А. Г. Остапенко. - Воронеж : ВИ МВД России, 2002. - 116 с. - ISBN 5-88591-002-4 : 20.00.	2002	50
Л2.5		Моделирование информационных операций и атак в сфере государственного и муниципального управления : Монография / под ред. В.И.Борисова. - Воронеж : ВИ МВД России, 2004. - 144 с. - Дар кафедры СИБ. - 100-00.	2004	25
Л2.6	Кулаков В.Г.; Кобяшев А.Б.; Андреев А.Б.; Линец А.Л.; Дидюк Ю.Е.; Макаров О.Ю.	Оптимальный синтез и анализ эффективности комплексов защиты информации : Монография. - Воронеж : ВГТУ, 2006. - 137 с. - 30-00.	2006	25
Л2.7	Дуров В.П.	Программно-аппаратная защита информации [Электронный ресурс] : учеб. пособие. -	2006	1

		Электрон. дан. (1 файл :6681088 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.		
Л2.8	Остапенко Г.А.	Логико-лингвистические модели атак на компьютерные системы [Электронный ресурс] : Учеб. пособие / под ред. А. Г. Остапенко. - Электрон. текстовые, граф. дан. (8452435 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.	2008	1
Л2.9	Пархоменко А.П. Мешкова А.Ф.; Менжулин Р.В.	Основные проблемы и особенности защиты информации в банковских системах: модели нарушителей [Электронный ресурс] / под ред. Г. С. Остапенко. - Электрон. текстовые, граф. дан. (1245435 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.	2008	1

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

Директор НТБ _____ / Т.И. Буковшина /

Контрольно-измерительные материалы для проведения текущего контроля и к зачету без оценки и с оценкой по дисциплине «Социальные сети: риски и обеспечение безопасности»

Контрольно-измерительные материалы текущего контроля

Вопросы текущего контроля:

7 семестр:

1. Что такое «социальная сеть»? Определение основных понятий
2. Механизмы, лежащие в основе функционирования социальных сетей
3. Свойства и метрики анализа сетей
4. Основные направления исследования компьютерных социальных сетей
5. Как моделировать влияние на основе информации об участниках
6. Как моделировать распространение влияния
7. Масштабно-инвариантные сети (scale-free networks).
8. Распределение Парето, нормализация, моменты.
9. Закон Ципфа.Граф ранк-частота.
10. Коэффициент кластерности
11. Методы анализа компьютерных социальных сетей
12. Основные направления исследования компьютерных социальных сетей
13. Модель Barabasi-Albert.
14. Модели "малого мира".
15. Модель Watts-Strogats.
16. Однопараметрическая модель.

8 семестр:

1. Понятия центральности и престижа.
2. Модельные графы.
3. Degree centrality, closeness centrality, betweenness centrality, статус/rank prestige (eigenvector centrality). Центральность сети.
4. Анализ связей. Алгоритм PageRank.
5. Стохастические матрицы. Теорема Perrona-Frobenius. Степенные итерации.
6. Нахождение собственного вектора. Hubs и Authorities.
7. Алгоритм HITS. Сравнение ранжировок.
8. Расстояние Kendall-Tau.
9. Метрики структурной эквивалентности узлов.
10. Эвклидово расстояние. Расстояние Хэмминга.
11. Корреляционный коэффициент. Сходство по косинусу). Ассортативное смешивание Модулярность Ассортативный коэффициент. Смешивание по степеням узлов
12. Понятие сетевых сообществ (network communities). Плотность связей. Метрики.
13. Разделение графа на части (graph partitioning).
14. Разрезы (cuts) в графе. Min-cut, quotent and normalized cuts метрики.
15. Divisive and agglomerative algorithms. Repeated bisection.
16. Корреляционная матрица. Классификация алгоритмов нахождения сообществ.
17. Edge Betweenness. Newman-Girvin. Спектральные методы. Максимизация модулярности (Newman)
18. Аппроксимационные алгоритмы.

19. Randomized min-cut (Karges's algorithm).
20. Multilevel алгоритмы. Metis алгоритм.
21. Локальная кластеризация. Conductance.
22. Алгоритм Nibble.
23. Нахождение структуры в графах.
24. Graph motiffs, k-cores, diad and triad census
25. Уравнение диффузии. Диффузия на сетях.
26. Дискретный оператор Лапласа, Матрица Лапласа, решение уравнения диффузии на графе. Случайные блуждания на графе.
27. Модели SI, SIR, SIS. Решения дифференциальных уравнений. Предельные случаи.
28. Модели SI, SIR, SIS на сетях. Приближенные решения дифференциальных уравнений на сетях. Предельные случаи. Иммунизация.
29. Пороговые модели принятия решений.
30. Granovetter's Threshold model коллективного поведения.
31. Определение наиболее влиятельных узлов.
32. Программные приложения для анализа социальных сетей
33. Модели формирования и роста сетей
34. Метрики структурной эквивалентности узлов.

9 семестр:

1. Обучение в сети.
2. Понятие консенсуса в сети.
3. Модель De Groot.
4. Условия достижимости консенсуса.
5. Условия возникновения информационных каскадов.
6. Модели каскадов
7. Модель сегрегации Шеллинга.
8. Сегрегация на сетях.
9. Условия возникновения сеграгации.
10. Информационные риски и эпистойкость безмасштабных сетей
11. Подходы к управлению эпистойкостью атакуемой безмасштабной сети

Контрольно-измерительные материалы зачета

1. Основные направления исследования компьютерных социальных сетей
2. Основные понятия в теории сетей. Основные измеряемые свойства сетей.
3. История исследования социальных сетей
4. Модели анализа социальных сетей
5. Степенное распределение. Распределение Парето, нормализация, моменты
6. Степенные законы для дискретных переменных.
7. Масштабно-инвариантные сети (scale-free networks).
8. Закон Ципфа. Граф ранк-частота.
9. Закон Хипса
10. Закономерность Бредфорда
11. Модель Эрдеша-Реньи
12. Наблюдения Барабаши-Альберт
13. Модель LCD
14. Модель Buckley-Osthus

15. Модель копирования
16. Модель Чунг-Лу
17. Модель Янсона-Лучака
18. Модель эпидемии SI
19. Модели просачивания и заражения
20. Модель распространения эпидемии, адаптированная к социальным информационным сетям
21. Риск-факторы безмасштабной сети
22. Подходы к управлению эпистойкостью атакуемой безмасштабной сети