МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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

«Математические модели информационного противоборства»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация «Обеспечение информационнной безопасности распределѐнных информационных систем»

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /Чопоров О.Н./

Заведующий кафедрой Систем информационной безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ /Остапенко А.Г./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины формирование у студентов профессиональных знаний о методах и моделях защиты информации в условиях информационного противоборства

1.2. Задачи освоения дисциплины

- изучить основные аспекты и модели информационного противоборства;
- изучить основные методы и средства защиты информации для информационных систем, находящихся в состоянии информационного конфликта;
- подготовить аспирантов к применению полученных знаний для анализа подсистемы информационной безопасности информационной системы и формирования модели управления информационной безопасностью объектов, находящихся в состоянии информационного конфликта.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Математические модели информационного противоборства» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Математические модели информационного противоборства» направлен на формирование следующих компетенций:

ПК-2 - способностью создавать и исследовать модели автоматизированных систем;

ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы;

ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-2	знать основные положения, современные и исторические концепции и математические структуры, используемые для создания и исследования моделей автоматизированных систем
	уметь создавать и исследовать модели автоматизированных систем
	владеть инструментальными средствами построения и анализа моделей автоматизированных систем
ПК-5	знать виды политик управления доступом и информационными потоками в автоматизированных системах
	уметь формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа
	владеть подходами к моделированию безопасности компьютерных систем, в том числе моделирования управления доступом и инфор-

	мационными потоками в компьютерных системах в условиях информационного противоборства
ПК-6	знать знает методологию менеджмента рисков информационной безопасности в автоматизированных системах
	уметь выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы в условиях информационного противоборства;
	владеет методами контроля эффективности принятых мер по реализации политик безопасности информации распределённых информационных системах в условиях информационного противоборства

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Математические модели информационного противоборства» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		5	6
Аудиторные занятия (всего)	134	54	80
В том числе:			
Лекции	76	36	40
Лабораторные работы (ЛР)	58	18	40
Самостоятельная работа	46	18	28
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 216 6	 72 2	 144 4

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	Лаб. зан.	СРС	Всего, час
1	Цели и задачи курса	Признаки информационной эпохи История информационных войн. Основные термины и определения. Концепция национальной безопасности РФ и задачи обеспечения безопасности. Нормативно-законодательное обеспечение информационной безопасности страны.	14	10	6	30
2	Понятие информационного противоборства в конфликтологии	Объекты и субъекты информационного противоборства. Особенности внешнего управления информационно-психологическими процессами. Информационно-психологическая агрессия. Понятие	14	10	8	32

		информационного оружия. Анализ использования технологий психологической войны.				
3	Социальные сети как среда информационного противоборства	Теоретико-игровые и имитационно-оптимизационные модели влияния и противоборства в социальных сетях. Стохастические модели социальных сетей. Марковская модель информационного влияния. Информационное управление и репутация членов сети. Распределѐнный контроль и согласование интересов.	12	10	8	30
4	Модели политик информационной безопасности	Модели политик информационной безопасности. Классификация существующих моделей политики ИБ. Модель дискреционного доступа (DAC). Модель безопасности Белла-Ла Падулы. Ролевая модель контроля доступа (RBAC)	12	10	8	30
5	Риск-моделирование информационного противоборства в информационных системах	Информационная система как объект атак. Методика анализа и регулирования рисков при реализации угроз доступа при информационном противоборстве в информационных системах. Оценка эффективности применения комплексов мер. Противодействия угрозам в процессе информационного противоборства в информационных системах	24	18	16	58
		Итого	**76**	**58**	**46**	**180**

5.2 Перечень лабораторных работ

1.Сбор данных из социальных сетей с помощью надстройки NodeXL для Excel.

2.Поиск лидеров мнений в Twitter с помощью надстройки NodeXL для Excel

3.Анализ хронологии распространения новости в Twitter.

4.Выявление интенсивности раскрутки или популярность той или иной новости/тренда.

5.Анализ тональности текста (Text Mining) на основе Orange3.

6.Поиск сообществ пользователей социальной сети

7.Измерение информационного влияния в социальной сети

8.Применение методов классификации и прогнозирования для выявления деструктивных сообщени в социальных сетях

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

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 6 семестре для очной формы обучения.

Примерная тематика курсового проекта:

Исследование возможностей влияния и особенностей противоборства в социальных сетях на основе:

Модели с порогами

Модели независимых каскадов

Модели просачивания и заражения

Модели Изинга
Модели на основе клеточных автоматов
Модели на основе цепей Маркова
Модели взаимной информированности
Модели согласованных коллективных действий
Модели коммуникаций Модели стабильности сети
Модели информационного влияния и управления
Модели информационного противоборства

Курсовой проект включат 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 шкал оценивания

7.1.1 Этап текущего контроля

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

«аттестован»; «не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-2	знать основные положения, современные и исторические концепции и математические структуры, используемые для создания и исследования моделей автоматизированных систем	знание основных положений, современных и исторических концепций и математические структуры, используемые для создания и исследования моделей автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь создавать и исследовать модели автоматизированных систем	умение создавать и исследовать модели автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть инструментальными средствами построения и анализа моделей автоматизированных систем	владение инструментальными средствами построения и анализа моделей автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	знать виды политик управления доступом и информационными потоками в автоматизированных системах	знание видов политик управления доступом и информационными потоками в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	умение формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	владеть подходами к моделированию безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах в условиях информационного противоборства	владение подходами к моделированию безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах в условиях информационного противоборства	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-6	знает методологию менеджмента рисков информационной безопасности в автоматизированных системах	знание методологии менеджмента рисков информационной безопасности в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы в условиях информационного противоборства;	умение выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы в условиях информационного противоборства;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеет методами контроля эффективности принятых мер по реализации политик безопасности информации распределённых информационных системах в условиях информационного противоборства	владение методами контроля эффективности принятых мер по реализации политик безопасности информации распределённых информационных системах в условиях информационного противоборства	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 5, 6 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-2	знать основные положения, современные и исторические концепции и математические структуры, используемые для создания и исследования моделей автоматизированных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь создавать и исследовать модели ав-	Решение стандартных практических задач	Продемонстрирован верный ход решения в большин-	Задачи не решены

	томатизированных систем		стве задач	
	владеть инструментальными средствами построения и анализа моделей автоматизированных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-5	знать виды политик управления доступом и информационными потоками в автоматизированных системах	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть подходами к моделированию безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах в условиях информационного противоборства	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-6	знать знает методологию менеджмента рисков информационной безопасности в автоматизированных системах	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы в условиях информационного противоборства;	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеет методами контроля эффективности принятых мер по реализации политик безопасности информации распределённых информационных системах в условиях информационного противоборства	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

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

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-2	знать основные положения, современные и исторические концепции и математические структуры, используемые для создания и исследования моделей автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь создавать и исследовать модели автоматизированных систем	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 не решены
	владеть инструментальными средствами построения и анализа моделей автоматизированных 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 не решены
ПК-5	знать виды политик управления доступом и информационными потоками в автоматизированных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	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 не решены
	владеть подходами к моделированию безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах в условиях информационного противоборства	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 не решены
ПК-6	знать знает методологию менеджмента рисков информаци-	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных

	онной безопасности в автоматизированных системах					ответов
	уметь выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы в условиях информационного противоборства;	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 не решены
	владеет методами контроля эффективности принятых мер по реализации политик безопасности информации распределённых информационных системах в условиях информационного противоборства	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 не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1. Примерный перечень заданий для решения стандартных задач

ПК-2 - способностью создавать и исследовать модели автоматизированных систем	
1.	Причины возникновения информационного противоборства
2.	Средства духовного воздействия в древности, используемые противоборствующими сторонами
3.	Способы ведения информационного противоборства в древности
4.	«Психологические операции» в Средние века
5.	Способы религиозного манипулирования
6.	Информационное противоборство во Второй мировой войне
7.	Идеология Победы России во второй мировой информационной войне
8.	Информационная война в современном мире
9.	Информационное оружие
10.	Социально-психологическая составляющая информационной войны
11.	Статус информационной составляющей в структуре современной цивилизации
12.	Информационная война против России и противостояние России информационной войне.
13.	Образ России в зеркале западных СМИ
14.	Методы манипулирования общественным сознанием в информационной войне
15.	Понятие и виды информационного оружия
ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	
1.	Концепция национальной безопасности РФ и задачи обеспечения безопасности

2.	Нормативно-законодательное обеспечение информационной безопасности страны
3.	Объекты и субъекты информационного противоборства
4.	Особенности внешнего управления информационно-психологическими процессами
5.	Модель распространения информационной угрозы (ИУ)
6.	Модель одновременного распространения нескольких видов информации (информационное противоборство)
7.	Влияние и индексы влиятельности
8.	Модели и свойства социальных сетей
9.	Стохастические модели социальных сетей: вырожденная социальная сеть
10.	Стохастические модели социальных сетей: невырожденная конечная социальная сеть
11.	Классификация существующих моделей политики ИБ.
12.	Информационное противоборство: распределённый контроль и согласование интересов
13.	Модели информационного управления и информационного противоборства: информационная эпидемия и защита от неё
14.	Имитационное моделирование информационного влияния и управления в социальных сетях
15.	Модели информационного управления и информационного противоборства: унифицированное информационное управление в однородных сетях. Роль СМИ
16.	Модели информационного управления и информационного противоборства: информационное управление и репутация членов сети
ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы	
1.	Информационная система как объект атак.
2.	Методика анализа и регулирования рисков при реализации угроз доступа при информационном противоборстве в информационных системах.
3.	Оценка эффективности применения комплексов мер противодействия угрозам в процессе информационного противоборства в информационных системах
4.	Формализованные модели информационных атак
5.	Анализ существующих моделей процесса обнаружения информационных атак
6.	Сигнатурные модели процесса обнаружения атак
7.	Поведенческие модели процесса выявления атак
8.	Модели процесса оценки рисков информационной безопасности АС
9.	Элементы теории защиты информации: объект, субъект, доступ. Основная аксиома теории защиты информации
10.	Понятие ролевого разграничения доступа. Базовая модель ролевого разграничения доступа
11.	Автоматная модель безопасности информационных потоков
12.	Виды политик безопасности. Общая характеристика дискреционной политики безопасности
13.	Классическая модель Белла-ЛаПадула мандатного разграничения доступа. Базовая теорема безопасности
14.	Виды политик безопасности. Общая характеристика мандатной политика безопасности.
15.	Похищение прав доступа в рамках модели *Take-Grant*

7.2.2. Примерный перечень заданий для решения прикладных задач

ПК-2 - способностью создавать и исследовать модели автоматизированных систем	
1	*Информационная война – это ...:* **А.** действия военных структур, направленные на достижение информационного превосходства при одновременном обеспечении собственной безопасности и защиты Б. любые действия, направленные на поддержку национальной военной стратегии путем воздействия на информацию и информационные системы противника при одновременном обеспечении собственной безопасности и защиты В. противоправные действия, направленные на достижение информационного превосходства путем активного воздействия на информацию и информационные системы противника с помощью недостоверной или неполной информации при одновременном обеспечении собственной безопасности и защиты Г. уничтожение или повреждение информационных систем противника Д. **любые действия, направленные на достижение информационного превосходства, на поддержку национальной военной стратегии путем активного воздействия на информацию и информационные системы противника для достижения поставленных целей при одновременном обеспечении собственной безопасности и защиты**
2	*Информационное оружие отличается от обычного ...* **А.** интеллектуальностью Б. **скрытностью** В. **масштабностью** Г. определенной последовательностью действий Д. **универсальностью**
3	*Целью информационной войны является:* **А. достижение информационного и информационно-технологического превосходства над противником** Б. нанесение ущерба информации, информационным процессам и информационным системам (ИТИ) противника В. одновременная защита собственной информации, информационных процессов и информационных систем (ИТИ)
4	*Стратегическими задачами информационной войны являются::* А. **нанесение ущерба информации, информационным процессам и информационным системам (ИТИ) противника** **Б.одновременная защита собственной информации, информационных процессов и информационных систем (ИТИ)** В. достижение информационного и информационно-технологического превосходства над противником
5	*Психологические операции как составные части информационной войны это?* А. **использование информации для воздействия на аргументацию солдат врага** Б. предоставление врагу ложную информацию о наших силах и намерениях В. прямое искажение информации без видимого изменения сущности, в которой она находится.
6	*Прямые информационные атаки, как составные части информационной войны это:* А. использование информации для воздействия на аргументацию солдат врага Б. предоставление врагу ложную информацию о наших силах и намерениях **В. прямое искажение информации без видимого изменения сущности, в которой она находится**
7	*К информационным средствам ведения информационной войны относятся?* **А. разведданные о состоянии критической (чувствительной) информации и**

	ИТИ противника; Б. информационно-вычислительные комплексы (включая суперкомпьютеры), системы и сети, предназначенные для нанесения ущерба государственно-значимой критической (чувствительной) информации и ИТИ противника; В. информационно-вычислительные комплексы (включая суперкомпьютеры), системы и сети, предназначенные для защиты собственной критической (чувствительной) информации и ИТИ
8	*К технологическим средствам ведения информационной войны относятся?* **А.** разведданные о состоянии критической (чувствительной) информации и ИТИ противника; **Б. информационно-вычислительные комплексы (включая суперкомпьютеры), системы и сети, предназначенные для нанесения ущерба государственно-значимой критической (чувствительной) информации и ИТИ противника;** **В. информационно-вычислительные комплексы (включая суперкомпьютеры), системы и сети, предназначенные для защиты собственной критической (чувствительной) информации и ИТИ**
9	*Отметьте верное высказывание. Экстремизм – это…* А. выдающиеся, экстраординарные действия, как правило, связанные с опасностью для жизни; **Б. приверженность к крайним взглядам и, в особенности, мерам;** В. целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам?
10	*Отметьте верное высказывание. Экстремизм – это…* А. выдающиеся, экстраординарные действия, как правило, связанные с опасностью для жизни; **Б. приверженность к крайним взглядам и, в особенности, мерам;** В. целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам
11	*Объектами воздействия в информационной войне выступают:* А. сети связи и информационно-вычислительные сети, используемые государственными Б. организациями при выполнении своих управленческих функций; В. военная информационная инфраструктура, решающая задачи управления войсками; информационные и управляющие структуры банков, транспортных и промышленных предприятий; Г. СМИ (в первую очередь электронные). **Д. все вышеперечисленные**
ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	
1	*Пороговая модель относится к классу оптимизационно-имитационных моделей влияния* **А. да** Б. нет
2	*Модель независимых каскадов относится к классу оптимизационно-имитационных моделей влияния* **А. да** Б. нет
3	*Модели просачивания и заражения относится к классу оптимизацион-*

	но-имитационных моделей влияния **А. да** Б. нет
4	*Модель Изинга относится к классу оптимизационно-имитационных моделей влияния* **А. да** Б. нет
5	*Модель на основе клеточных автоматов относится к классу оптимизационно-имитационных моделей влияния* **А. да** Б. нет
6	*Модель на основе Марковских цепей относится к классу оптимизационно-имитационных моделей влияния* **А. да** Б. нет
7	*Модель взаимной информированности относится к классу теоретико-игровых моделей влияния* **А. да** Б. нет
8	*Модель согласованных коллективных действий относится к классу теоретико-игровых моделей влияния* **А. да** Б. нет
9	*Модель коммуникаций относится к классу теоретико-игровых моделей влияния* **А. да** Б. нет
10	*Модель информационного влияния и управления относится к классу теоретико-игровых моделей влияния* **А. да** Б. нет
11	*Модель информационного противоборства относится к классу теоретико-игровых моделей влияния* **А. да** Б. нет
12	*Модель Изинга это* **А. *математическая модель, описывающая возникновение намагничивания материала*** Б. модель распространения эпидемии, основанная на цикле заболевания носителя В. модель распространения эпидемии, основанная на цикле заболевания носителя
13	*Модель на основе клеточных автоматов – это:* **А.** математическая модель, описывающая возникновение намагничивания материала Б. модель распространения эпидемии, основанная на цикле заболевания носителя В. **модель, представляющая набора объектов (агентов) в виде регулярной решетки и состояние отдельно взятого агента в каждый дискретный момент времени характеризуется некоторой переменной. Рассматриваемые состояния объекта синхронно изменяются через дискретные интервалы времени в соответствии с неизменными локальными вероятностными правилами, которые могут зависеть от состояния переменных, описывающих ближайших соседних агентов в окрестности данного агента, а также возможно, от**

	состояния самого агента
14	*В основе модели Харрисона-Рузо-Ульмана лежит _____ политика безопасности* **А. дискреционная** Б. мандатная В. ролевая
15	*В основе модели Белла-Ла-Падулы лежит _____ политика безопасности* А. дискреционная **Б. мандатная** В. ролевая
16	*В основе модели типизованной матрицы доступа лежит _____ политика безопасности* **А.дискреционная** Б.мандатная В. Ролевая
17	*В основе модели TAKE-GRANT лежит _____ политика безопасности* **А. дискреционная** Б. мандатная В. ролевая
18	*Произвольное (дискреционное) управление доступом основывается на* **А. атрибутах безопасности (FDP_ACF.1)** Б. иерархических атрибутах безопасности (FDP_IFF.2) В. управлении информационными потоками (FDP_IFC.1)
19	*К моделям КС с дискреционным управлением доступом относятся:* **А. модель матрицы доступов Харрисона-Рузо-Ульмана** Б. модель Белла-ЛаПадулы В. автоматная модель безопасности информационных потоков Г. вероятностная модель контроля информационных потоков
20	*Математические понятия, относящиеся к моделям безопасности:* *(несколько вариантов ответов)* А. **граф;** **Б. автомат;** **В. решётка;** Г. дифференциальное уравнения Д. уравнение в конечных разностях.
	Дайте правильное определение основной аксиомы компьютерной безопасности: А. **в рамках субъект сущностного подхода все вопросы безопасности информации в КС описываются доступами субъектов к сущностям;** Б. информационным потоком от сущности к источнику к сущности-приемнику называется преобразование данных в сущности-приемнике; В. все действия в КС, в том числе выполнение операций над сущностями, могут быть инициированы только субъектами КС с использованием доступов к сущностям КС.
	Правилами (де-юре) классической модели Take-Grant являются: (несколько вариантов ответов) А. ***take*** Б. ***grant*** ***В. crteate*** Г. ***remove*** Д. delete Е. post Ж. pass

	3. spy
	Стоимость правила в модели Take-Grant может: **А. являться константой** Б. не зависеть от специфики правила В. зависеть от степени требуемого взаимодействия и не зависеть от числа и состава участников при применении правила
ПК-5 - способностью проводить анализ рисков информационной безопасности автоматизированной системы	
1	*Что в сфере информационной безопасности принято считать риском* **А. потенциальную возможность понести убытки из-за нарушения безопасности информационной системы** Б. потенциально возможное происшествие неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на компьютерную В. систему, а также информацию, хранящуюся и обрабатывающуюся в ней характеристику, которая делает возможным возникновение угрозы
2	*2. Что принято считать ресурсом или активом информационной системы?* А. модель информационной системы Б. все элементы, имеющие материальную ценность независимо от того подлежат они защите или нет **В. именованный элемент информационной системы, имеющий (материальную) ценность и подлежащий защите**
3	*Что отличает риск от угрозы?* А. объем вероятных потерь **Б. наличие количественной оценки возможных потерь и (возможно)** **В. оценки вероятности реализации угрозы** Г. угроза и риск - понятия идентичные
4	*Почему аналитический метод определения минимальных затрат при расчетах защиты информационной системы неприменим?* А. потому, что расчеты ресурсов подвержены флуктуациям, связанными с колебаниями на рынке услуг в сфере безопасности ИС **Б. потому, что на практике точные зависимости между затратами и уровнем защищенности определить не представляется возможным** В. потому, что уровень защищенности информационной системы неадекватен затратам на ее защиту
5	*Идентифицируется ли риск уязвимостью, через которую может быть реализована некая угроза в отношении определенного ресурса?* **А. да** Б. нет В. да, но только в случае отсутствия угрозы
6	*Какие из перечисленных характеристик не входят в систему обеспечения безопасности Клементса: О - набор защищаемых объектов; Т - набор угроз; М - набор средств обеспечения безопасности; Р- набор креативных функций; Z - набор виндикативных инструментов?* **А. О - набор защищаемых объектов; Т - набор угроз; М - набор средств обеспечения безопасности; Р- набор креативных функций** Б. О - набор защищаемых объектов; Т - набор угроз; М - набор средств обеспечения безопасности; Р- набор креативных функций; Z - набор виндикативных инструментов В. Р- набор креативных функций; Z - набор виндикативных инструментов
7	*В каком отечественном документе впервые в России выделено понятие риска в отношении ИБ?*

	А. ГОСТ Р ИСО/МЭК 15408-2002 Б. КЗОТ В. УК РФ
8	*Какой термин определяет характеристику функции безопасности объекта оценки, выражающую минимальные усилия, которых теоретически может быть достаточно для нарушения работоспособности при прямой атаке на информационную систему?* А. "потенциал падения" **Б. "стойкость функции безопасности (СФБ)"** В. "резистивность системы" (РС)
9	*Что представляет собой событие - триггер?* **А. событие, повлекшее реализацию или дальнейшее развитие рисков и являющееся идентификатором риска** Б. событие, увеличивающее время отклика web – сервера В. это одна из разновидностей атак на сервер
10	*Какой из перечисленных вариантов последовательности действий предписан стандартом ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью" в аспектах управления непрерывностью бизнеса?* **А. идентифицировать события, которые могут быть причиной прерывания бизнес-процессов, провести оценку последствий, после чего разработать планы восстановления;** Б. произвести экспертную оценку контента информации на сервере на предмет возможных схем утечки критически важной информации, после чего разработать планы восстановления системы; В. произвести контроль плана восстановления и его тестирование на предмет реализуемости, затем идентифицировать события, которые могут быть причиной прерывания бизнес-процессов (отказ оборудования, пожар и т.п.)
11	*С какой целью при разработке и реализации политики безопасности используются метрики?* А. для определения рамок, в которых осуществляются мероприятия по обеспечению безопасности информации, и задаются критерии оценки полученных результатов Б. для замеров уровней безопасности **В. с целю определения параметров защищенности системы, что позволяет соотнести сделанные затраты и полученный эффект**
12	*Какая из перечисленных распространенных методик анализа рисков использует метод оценки риска на качественном уровне (например, по шкале "высокий", "средний", "низкий")?* А. FRAP Б. RiskWatch **В. CRAMM +**
13	*Какая из перечисленных распространенных методик анализа рисков использует количественные методики оценки рисков?* А. FRAP Б. **RiskWatch +** В. CRAMM Microsoft
14	*Какие из перечисленных распространенных методик анализа рисков используют смешанный метод оценки риска?* **А. CRAMM** **Б. Microsoft**

	В. RiskWatch Г. FRAP

7.2.3. Примерный перечень вопросов для подготовки к зачету

Признаки информационной эпохи. История информационных войн.

Основные термины и определения. Концепция национальной безопасности РФ и задачи обеспечения безопасности. Нормативно-законодательное обеспечение информационной безопасности страны.

Объекты и субъекты информационного противоборства. Особенности внешнего управления информационно-психологическими процессами. Информационно-психологическая агрессия. Понятие информационного оружия. Анализ использования технологий психологической войны.

Теоретико-игровые и имитационно-оптимизационные модели влияния и противоборства в социальных сетях. Стохастические модели социальных сетей. Марковская модель информационного влияния. Информационное управление и репутация членов сети. Распределѐнный контроль и согласование интересов.

Модели политик информационной безопасности. Классификация существующих моделей политики ИБ.

Модель дискреционного доступа (DAC). Модель безопасности Белла-Ла Падулы. Ролевая модель контроля доступа (RBAC)

Информационная система как объект атак. Методика анализа и регулирования рисков при реализации угроз доступа при информационном противоборстве в информационных системах. Оценка эффективности применения комплексов мер. Противодействия угрозам в процессе информационного противоборства в информационных системах

7.2.4. Примерный перечень заданий для решения прикладных задач

1.Признаки информационной эпохи История информационных войн. Основные термины и определения. Концепция национальной безопасности РФ и задачи обеспечения безопасности. Нормативно-законодательное обеспечение информационной безопасности страны.

2.Объекты и субъекты информационного противоборства. Особенности внешнего управления информационно-психологическими процессами.

3.Информационно-психологическая агрессия. Понятие информационного оружия. Анализ использования технологий психологической войны.

4.Теоретико-игровые и имитационно-оптимизационные модели влияния и противоборства в социальных сетях.

5.Стохастические модели социальных сетей. Марковская модель информационного влияния.

6.Информационное управление и репутация членов сети. Распределѐнный контроль и согласование интересов.

7. Модели политик информационной безопасности. Классификация существующих моделей политики ИБ.

6. Модель дискреционного доступа (DAC).

7. Модель безопасности Белла-Ла Падулы.

8. Ролевая модель контроля доступа (RBAC)

9. Информационная система как объект атак.

10. Методика анализа и регулирования рисков при реализации угроз доступа при информационном противоборстве в информационных системах.

11.Оценка эффективности применения комплексов мер противодействия угрозам в процессе информационного противоборства в информационных система*х*

7.2.5. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное 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.)

7.2.6. Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Цели и задачи курса	Цели и задачи курса	Тест, контрольная работа, защита лабораторных работ, требования к курсовому проекту
2	Понятие информационного противоборства в конфликтологии	Понятие информационного противоборства в конфликтологии	Тест, контрольная работа, защита лабораторных работ, требования к курсовому проекту
3	Социальные сети как среда информационного противоборства	Социальные сети как среда информационного противоборства	Тест, контрольная работа, защита лабораторных работ, требования к курсовому проекту
4	Модели политик информационной безопасности	Модели политик информационной безопасности	Тест, контрольная работа, защита лабораторных работ, требования к курсовому проекту
5	Риск-моделирование информационного противоборства в информационных системах	ПК-2, ПК-23	Тест, контрольная работа, защита лабораторных работ, требования к курсовому проекту

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 методики 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 методики 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 методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик 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

Остапенко А.Г.Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс] : Учеб.пособие. - Электрон.текстовые, граф. дан. (112 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

Дополнительная литература

1.Методические указания к самостоятельным работам по дисциплинам «Математические модели информационного противоборства», «Математическое моделирование информационных операций и атак» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост.: О. Н. Чопоров, Е. А. Шварцкопф. - Электрон.текстовые, граф. дан. (262 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

2.Губанов Д.А. Социальные сети. Модели информационного влияния, управления и противоборства [Электронный ресурс]: учебное пособие/ Гу-

банов Д.А., Новиков Д.А., Чхартишвили А.Г.— Электрон.текстовые данные.— Москва: Издательство физико-математической литературы, 2010.— 228 с.— Режим доступа: http://www.iprbookshop.ru/8531.html.— ЭБС «IPRbooks».

3. Новиков Д.А. Прикладные модели информационного управления [Электронный ресурс]: монография/ Новиков Д.А., Чхартишвили А.Г.— Электрон.текстовые данные.— Москва: ИПУ РАН, 2004.— 129 с.— Режим доступа: http://www.iprbookshop.ru/8518.html.— ЭБС «IPRbooks».

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного 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/
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

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 «Математические модели информационного противоборства» 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 пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	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 промежуточной аттестации.
Подготовка к промежуточной аттестации	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.