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

«Информационное противоборство в мультисетевом пространстве»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ /А.Т. Остапенко/

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

Руководитель ОПОП _____ /А.Т. Остапенко/

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1. Целидисциплины

Изучение подходов к определению информационного противоборства в мультисетевом пространстве, как составной части национальной безопасности любого государства с учѐтом новых методов и средств взаимодействия противоборствующих сторон.

1.2. Задачиосвоениядисциплины

- познакомить студентов с формами информационной борьбы «второго» поколения, связанными с использованием в качестве информационной инфраструктуры мультисетевого пространства как арены организации противодействия;
- сформировать у студентов устойчивую систему взглядов на необходимость повышения эффективности ведения информационного взаимодействия в мультисетевом пространстве с учѐтом современных видов, методов и средств организации и ведения кибервойн

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Информационноепротивоборствовмультисетевомпространстве»относитсякдисциплинамвариативнойчастиблокаФТД.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Информационноепротивоборствовмультисетевомпространстве»направленнаформированиеследующихкомпетенций:

ПК-5-способностьюпроводитьанализрисковинформационнойбезопасностиавтоматизированнойсистемы

ПК-11-способностьюразрабатыватьполитикуинформационнойбезопасностиавтоматизированнойсистемы

ПК-17-способностьюпроводитьинструментальныймониторингзащищенностиинформациивавтоматизированнойсистемеивыявлятьканалыутечкиинформации

ПК-22-способностьюучаствоватьвформированииполитикиинформационнойбезопасностиорганизацииконтролироватьэффективностьеереализации

ПСК-7.2-способностьюпроводитьанализрисковинформационнойбезопасностииразрабатывать,руководитьразработкойполитикибезопасностивраспределенныхинформационныхсистемах

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ПК-5	Знать: - основные риски информационной безопасности в мультисетевом пространстве; - основные этапы анализа рисков информационной безопасности в мультисетевом пространстве.

	Уметь: - рассчитывать риски информационной безопасности в условиях сетевого противоборства; -разрабатывать методику анализа рисков информационной безопасности в мультисетевом пространстве.
	Владеть: -рассчетами рисков информационной безопасности в условиях сетевого противоборства; - разработкой методики анализа рисков информационной безопасности в мультисетевом пространстве.
ПК-11	Знать: -основные составляющие политики безопасности; - принципы разработки политики безопасности.
	Уметь: - разрабатывать политику безопасности; - применять комплексный подход к обеспечению информационной безопасности в условиях информационного противоборства.
	Владеть: -навыками разработки политики безопасности; -способностью применения комплексного подхода к обеспечению информационной безопасности в условиях информационного противоборства.
ПК-17	Знать: - методику анализа информационной безопасности; - современные стандарты в области информационной безопасности.
	Уметь: -разрабатывать методику анализа информационной безопасности; - использовать стандарты в области информационной безопасности.
	Владеть: - разработкой анализа информационной безопасности; -умением использования стандартов в области информационной безопасности.
ПК-22	Знать: -основные составляющие политики безопасности; - принципы разработки политики безопасности.
	Уметь: - разрабатывать политику безопасности.

	- применять комплексный подход к обеспечению информационной безопасности.
	Владеть: - навыками разработки политики безопасности; - способностью применения комплексного подхода к обеспечению информационной безопасности.
ПСК-7.2	Знать методики проведения анализа рисков информационной безопасности
	уметь разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Информационноепротивоборствовмультисетевомпространстве»составляет2з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

очнаяформаобучения

Видыучебнойработы	Всегочасов	Семестры
		9
Аудиторныезанятия (всего)	54	54
В томчисле:		
Лекции	36	36
Практическиезанятия (ПЗ)	18	18
Самостоятельнаяработа	18	18
Видыпромежуточнойаттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 72 2	 72 2

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ зан.	СРС	Всего, час
1	СТРАТЕГИЯ ОБЕСЦЕНИВАНИЯ И ВЗВЕШЕННЫЕ СЕТИ на примере НЕФТЯНОЙ ОТРАСЛИ	Структура нефтяной сети Российской Федерации Нефтяная инфраструктура Российской федерации. Основные пункты переработки и транспортировки российской нефти. Рассмотрениеориентированных и неориентированных взвешенных графов нефтяной сети Российской Федерации.	6	2	2	10
2	Моделирование сетевой атаки на нефтяную	Стратегический ресурс сети. Динамический ресурс сети.	6	2	2	10

	отрасль	Ресурс всей сети. Снижение цены на нефть как целенаправленная стратегия сетевого противоборства.				
3	Управление валютным курсом в условиях атак на нефтяную сеть	Стратегии управления курсом национальной валюты. Плавающий курс валюты. Массированные атаки и стратегия устранения.	6	2	2	10
4	СТРАТЕГИЯ УСТРАНЕНИЯ И ВЗВЕШЕННЫЕ БЕСПРОВОДНЫЕ ИНФОРМАЦИОННЫЕ СЕТИ	Живучесть атакуемых сетевых структур при блокировании их элементов Оценка ущерба. Оценка пользы. Временная зависимость динамического ресурса вершины сети при атаке без восстановления. Временная зависимость динамического ресурса вершины сети при атаке с восстановлением.	6	4	4	14
5	Структурно-функциональная специфика блокирования элементов атакуемой беспроводной сети	Беспроводные сети, их иерархическая система. Методы и актуальные атаки блокирования элементов сети, их классификация. Риск-анализ реализации данных методов и разработка соответствующих мер противодействия на примере сотового оператора.	6	4	4	14
6	2.3 Риск-анализ блокирования элементов беспроводной сети	Составляющие рисков блокирования элементов для уровней иерархии сети. Оценка эффективности применяемых средств защиты в условиях реализации угроз блокирования элементов сети.	6	4	4	14
		Итого	36	18	18	72

5.2 Перечень лабораторных работ

Непредусмотреноучебнымпланом

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыполнениекурсовогопроекта(работы)иликонтрольнойработы.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-5	знать	знание основных рисков	Выполнение работ в	Невыполнение

	-: основные риски информационной безопасности в мультисетевом пространстве; - основные этапы анализа рисков информационной безопасности в мультисетевом пространстве.	информационной безопасности в мультисетевом пространстве; основных этапов анализа рисков информационной безопасности в мультисетевом пространстве	срок, предусмотренный в рабочих программах	работ в срок, предусмотренный в рабочих программах
	уметь - рассчитывать риски информационной безопасности в условиях сетевого противоборства; - разрабатывать методику анализа рисков информационной безопасности в мультисетевом пространстве.	умение рассчитывать риски информационной безопасности в условиях сетевого противоборства; разрабатывать методику анализа рисков информационной безопасности в мультисетевом пространстве	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть -рассчетами рисков информационной безопасности в условиях сетевого противоборства; - разработкой методики анализа рисков информационной безопасности в мультисетевом пространстве.	владение - расчётами рисков информационной безопасности в условиях сетевого противоборства; - разработкой методики анализа рисков информационной безопасности в мультисетевом пространстве.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-11	знать - основные составляющие политики безопасности; - принципы разработки политики безопасности.	знаниеосновных составляющие политики безопасности; принципы разработки политики безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - разрабатывать политику безопасности; - применять комплексный подход к обеспечению информационной безопасности в условиях информационного противоборства.	умениеполитику безопасности; - применять комплексный подход к обеспечению информационной безопасности в условиях информационного противоборства.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть -: навыками разработки политики безопасности; - способностью	владение навыками разработки политики безопасности; способностью применения комплексного подхода к	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	применения комплексного подхода к обеспечению информационной безопасности в условиях информационного противоборства.	обеспечению информационной безопасности в условиях информационного противоборства.		
ПК-17	знать - методику анализа информационной безопасности; - современные стандарты в области информационной безопасности.	Знание методики анализа информационной безопасности, а также современные стандарты в области информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - разрабатывать методику анализа информационной безопасности; -: использовать стандарты в области информационной безопасности.	умение разрабатывать методику анализа информационной безопасности и использовать стандарты в области информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть -: разработкой анализа информационной безопасности; - умением использования стандартов в области информационной безопасности.	владениеразработкой анализа информационной безопасности, умением использования стандартов в области информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-22	знать - основные составляющие политики безопасности; -: принципы разработки политики безопасности.	знание основных составляющих политики безопасности, принципов разработки политики безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь - разрабатывать политику безопасности. -: применять комплексный подход к обеспечению информационной безопасности.	умение разрабатывать политику безопасности. и применять комплексный подход к обеспечению информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть - навыками разработки политики безопасности; - способностью применения комплексного подхода к обеспечению	Владение навыками разработки политики безопасности и способностью применения комплексного подхода к обеспечению информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	информационной безопасности.			
ПСК-7.2	Знать методики проведения анализа рисков информационной безопасности	знаниеметодики проведения анализа рисков информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	умение разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв9семестредля очнойформыобученияподвухбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
ПК-5	знать - основные риски информационной безопасности в мультисетевом пространстве; - основные этапы анализа рисков информационной безопасности в мультисетевом пространстве.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь - рассчитывать риски информационной безопасности в условиях сетевого противоборства; - разрабатывать методику анализа рисков информационной безопасности в мультисетевом пространстве.	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	владеть -рассчетами рисков информационной безопасности в условиях сетевого противоборства; - разработкой методики анализа рисков информационной безопасности в мультисетевом	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены

	пространстве.			
ПК-11	знать - основные составляющие политики безопасности; - принципы разработки политики безопасности.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь - разрабатывать политику безопасности; - применять комплексный подход к обеспечению информационной безопасности в условиях информационного противоборства.	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
	владеть - навыками разработки политики безопасности; - способностью применения комплексного подхода к обеспечению информационной безопасности в условиях информационного противоборства.	Решение прикладных задач в конкретной предметной области	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
ПК-17	знать - методику анализа информационной безопасности; - современные стандарты в области информационной безопасности.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь - разрабатывать методику анализа информационной безопасности; - использовать стандарты в области информационной безопасности.	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
	владеть - разработкой анализа информационной безопасности; - умением использования стандартов в области информационной безопасности.	Решение прикладных задач в конкретной предметной области	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены

ПК-22	знать - основные составляющие политики безопасности; - принципы разработки политики безопасности.	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь - разрабатывать политику безопасности. - применять комплексный подход к обеспечению информационной безопасности.	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
	владеть - навыками разработки политики безопасности; - способностью применения комплексного подхода к обеспечению информационной безопасности.	Решение прикладных задач в конкретной предметной области	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
ПСК-7.2	Знать методики проведения анализа рисков информационной безопасности	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	уметь разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданиялииныематериалы,необходимыедляоценкизнаний,умений,навыкови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1) Виды информационной безопасности:

+ Персональная, корпоративная, государственная

- Клиентская, серверная, сетевая

- Локальная, глобальная, смешанная

2) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации

- Техническое вмешательство, выведение из строя оборудования сети

+ Потеря, искажение, утечка информации

3) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети

- инсайдерства в организации

- чрезвычайных ситуаций

4) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности

- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

5) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
6) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
7) Политика безопасности строится на основе:
-общих представлений об ИС организации;
- изучения политик родственных организаций;
+ анализа рисков**.**
8) Управление рисками включает в себя следующие виды деятель ности:
- определение ответственных за анализ рисков;
+ оценка рисков;
+ выбор эффективных защитных средств.

9) К современным стандартам в области информационной безопасности относятся:

+ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"
-2. ГОСТ Р ИСО/МЭК 17799:2016 "Информационная технология. Практические правила управления информационной безопасностью"
+ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

10) Проранжируйте по времени основные этапы, проводимые при анализе риска безопасности ИС

- Определение уязвимых мест ИС.
Оценка ожидаемых размеров потерь.
Оценка выгоды от применения предполагаемых мер.
Описание компонентов ИС.
Оценка вероятностей проявления угроз безопасности ИС.
Обзор возможных методов защиты и оценка их стоимости.
- Описание компонентов ИС.
Оценка вероятностей проявления угроз безопасности ИС.
Обзор возможных методов защиты и оценка их стоимости. Определение уязвимых мест ИС.
Оценка ожидаемых размеров потерь.
Оценка выгоды от применения предполагаемых мер.
- *Описание компонентов ИС.*
Определение уязвимых мест ИС.
Оценка вероятностей проявления угроз безопасности ИС.
Оценка ожидаемых размеров потерь.
Обзор возможных методов защиты и оценка их стоимости.
Оценка выгоды от применения предполагаемых мер.
- Описание компонентов ИС.
Определение уязвимых мест ИС. 47336 32
Оценка вероятностей проявления угроз безопасности ИС.
Обзор возможных методов защиты и оценка их стоимости.
Оценка ожидаемых размеров потерь.
Оценка выгоды от применения предполагаемых мер

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач
(минимум10вопросовдлятестированиясвариантамиответов)
7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач
(минимум10вопросовдлятестированиясвариантамиответов)
7.2.4Примерныйпереченьвопросовдляподготовкикзачету
Укажитевопросыдлязачета
7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач
Непредусмотреноучебнымпланом
7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации
(Например:Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсо

держит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5баллов заверныйответ).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабрал менее6баллов.

2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабрало т6до10баллов

3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы) дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Структура нефтяной сети Российской Федерации	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Моделирование сетевой атаки на нефтяную отрасль	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Управление валютным курсом в условиях атак на нефтяную сеть	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Живучесть атакуемых сетевых структур при блокировании их элементов	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Структурно-функциональная специфика блокирования элементов атакуемой беспроводной сети	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Риск-анализ блокирования элементов беспроводной сети	ПК-5, ПК-11, ПК-17, ПК-22, ПСК-7.2	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении

промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведенииипромежуточнойаттестации.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

1. Остапенко, А.Г.Обнаружение и нейтрализация вторжений в распределенных информационных системах [Электронный ресурс] : Учеб.пособие / А. Г. Остапенко, М. Н. Иванкин. - Электрон.текстовые, граф. дан. (366 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

2. Остапенко О.А.Риски систем: Оценка и управление [Электронный ресурс] : учеб.пособие / О. А. Остапенко, Д. О. Карпеев, В. Н. Асеев. - Электрон.дан. (1 файл :5250 Кбайта). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.

3. Кушнир, А.Э.Рефлексивные игры в информационном пространстве социотехнических систем [Электронный ресурс] : Учеб.пособие / А. Э. Кушнир, О. А. Остапенко, И. В. Сысоев. - Электрон.текстовые дан. (3 230 235 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.

Дополнительная литература:

1. Демьяненко, Н.Ю.Информационно-психологические воздействия в открытых информационно-телекоммутационных системах [Электронный ресурс] : Учеб.пособие / Н. Ю. Демьяненко. - Электрон.текстовые дан. (1 652 654 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.

2. Остапенко Г.А.Информационные операции [Электронный ресурс] : учеб.пособие / Г. А. Остапенко, Е. А. Мешкова. - Электрон.дан. (1 файл :3045 Кбайта). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2006. - 1 файл. - 30-00.

3. Остапенко, О.А. Опасность, ущербы и риски систем : Учеб.пособие / О. А. Остапенко, Р. В. Батищев. - Воронеж : НОУВПО "Междунар. ин-т компьют. технологий", 2007. - 194 с. - 45-00.

8.2Переченьинформационныхтехнологий,используемыхприосуществлениииобразовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

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)

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

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

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Информационноепротивоборствовмультисетевомпространстве»читаютсялекции,проводятсяпрактическиезанятия.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Практическиезанятиянаправленынаприобретениепрактическихнавыковрасчета_____.Занятияпроводятсяпутемрешенияконкретныхзадачваудитории.

Видучебныхзанятий	Деятельностьстудента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельнаяработа	Самостоятельная работа студентов способствует глубокому

	усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточнойаттестации.
Подготовка к промежуточнойаттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.