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

«Информационные конфликты и противоборство в сетевых структурах»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация «Безопасность распределённых компьютерных систем»

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /Остапенко А.Г./

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

Руководитель ОПОП _____ / Остапенко А.Г./

Воронеж 2017

1.1. Цели дисциплины

Изучение подходов к определению информационного противоборства в мультисетевом пространстве

1.2. Задачи освоения дисциплины

- познакомить студентов с формами информационной борьбы «второго» поколения,
- сформировать у студентов устойчивую систему взглядов на необходимость повышения

Процесс изучения дисциплины «Информационное противоборство в мультисетевом пространстве» направлен на формирование компетенций:

ПК-12- способностью проводить инструментальный мониторинг защищенности компьютерных систем

ПК-15- способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы

ПСК-3.1 способностью использовать современные критерии и стандарты для анализа безопасности распределенных компьютерных систем

ПСК-3.4- способностью организовывать защиту информации в распределенных компьютерных системах

1. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Информационные конфликты противоборство в мультисетевом пространстве» составляет 7 з.е.

Распределение трудоемкости дисциплины по видам занятий

Очная форма обучения

Виды учебной работы	Всегочасов	Семестры	
		9	10
Аудиторные занятия (всего)	90	54	36
В том числе:			
Лекции	54	36	18
Лабораторные работы (ЛР)	36	18	18
Самостоятельная работа	126	36	90
Курсовой проект	+		+
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 252 7	 90 2.5	 162 4.5

5.1 Содержаниеразделовдисциплиныираспределениетрудоемкости повидам

п/п	Наименованиетемы
	СТРАТЕГИЯ ОБЕСЦЕНИВАНИЯ И ВЗВЕШЕННЫЕ СЕТИ на примере НЕФТЯНОЙ ОТРАСЛИ
	Моделирование сетевой атаки на нефтяную отрасль
	Управление валютным курсом в условиях атак на нефтяную сеть
	СТРАТЕГИЯ УСТРАНЕНИЯ И ВЗВЕШЕННЫЕ БЕСПРОВОДНЫЕ ИНФОРМАЦИОННЫЕ СЕТИ

	Структурно-функциональная специфика блокирования элементов атакуемой беспроводной сети
	2.3 Риск-анализ блокирования элементов беспроводной сети

5.2 Переченьлабораторныхработ

Не предусмотрено учебным планом

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение лабораторных работ

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах контроля

7.2. 7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестациионенива ютсяп

«аттестован»;

«неаттестован».

Компе- тенция	**Результатыобучения,характеризу сформированностькомпетенц**
ПК-12	знать: – принципы работы элементов и функциональных узлов комп условиях информационного противоборства;
	уметь проводить анализ качества показателей компьютерных систем
	владеть - навыками анализа основных характеристик и использован экспериментальном исследовании компьютерных систем.
ПК-15	знать -основные понятия и последовательность этапов решени необходимых для совершенствования системы управлен компьютерной системы;
	уметь - определить математический аппарат, необходимый для реш управления в рамках динамической системы управления без условиях информационного противоборства в мультисетевом п
	владеть - методиками построения линейных оптимальных систем управ компьютерной системы и их реализациями в современных ин инженерных и научных расчѐтов
ПСК-3.1	знать - современные критерии оценки риска и стандарты дляанализабезопасностираспределенныхкомпьютерныхсистем

	рисками
	уметь - применять на практике подходы к аналитическом оце нерегулярности распределения ущербов и их динамики
ПСК-3.4	знать - способы организации защиты информации в компьютерных противоборства в мультисетевом пространстве
	уметь - проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных
	владеть -инструментальными средствами проведения мониторинга и защищенности КС

7.1.2Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 8 семестре для очной формы обучения

«зачтено»

«незачтено»

Компе- тенция	**Результатыобучения,характеризу сформированностькомпетенц**
ПК-12	знать: – принципы работы элементов и функциональных узлов комп условиях информационного противоборства;
	уметь проводить анализ качества показателей компьютерных систем
	владеть - навыками анализа основных характеристик и использован экспериментальном исследовании компьютерных систем.
ПК-15	знать -основные понятия и последовательность этапов решени необходимых для совершенствования системы управлен компьютерной системы;
	уметь - определить математический аппарат, необходимый для реш управления в рамках динамической системы управления без условиях информационного противоборства в мультисетевом п
	владеть - методиками построения линейных оптимальных систем управ компьютерной системы и их реализациями в современных ин инженерных и научных расчѐтов
ПСК-3.1	знать - современные критерии оценки риска и стандарты дляанализабезопасностираспределенныхкомпьютерныхсистем рисками
	уметь - применять на практике подходы к аналитическом оце нерегулярности распределения ущербов и их динамики

ПСК-3.4	знать - способы организации защиты информации в компьютерных противоборства в мультисетевом пространстве
	уметь - проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных
	владеть -инструментальными средствами проведения мониторинга и защищенности КС

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезадания7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

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, предуп

+ 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 перечисленные

+ 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

-2. ГОСТ Р ИСО/МЭК 17799:2016 "Информационная технология. Практически

+ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и сре

10) Проранжируйте по времени основные этапы, проводимые при анализе рисков

•

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 уязви 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

7.2.2Примерный перечень заданий для решения стандартных задач *указаны в ОМ по дисциплине*

7.2.3 Примерный перечень заданий для решения прикладных задач *указаны в ОМ по дисциплине*

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

указаны в ОМ по дисциплине

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

Не предусмотрено учебным планом

7.2.6.Методикавыставленияоценкипripроведенииипромежуточнойаттеста

(Например:Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержи еколичествонабранныхбаллов–20.

1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6
2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10б
3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.

4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемые разделы
1	Структура нефтяной сети Российской Федерации
2	Моделирование сетевой атаки на нефтяную отрасль
3	Управление валютным курсом в условиях атак на нефтяную сеть
4	Живучесть атакуемых сетевых структур при блокировании их эле
5	Структурно-функциональная специфика блокирования элементов
6	Риск-анализ блокирования элементов беспроводной сети

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

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

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценки

припроведенииипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютерн ойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномно сителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязада чэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкип рипроведенииипромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампракт икосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымв методическихматериалах.Примерноевремязащитынаодногостудентасоставля ет20мин.

8.1 Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

1. Остапенко, А.Г. Обнаружение и нейтрализация вторжений в распределе "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.
2. Остапенко О.А. Риски систем: Оценка и управление [Электронный ресу университет", 2006. - 1 файл. - 30-00.
3. Кушнир, А.Э. Рефлексивные игры в информационном пространстве соц "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.

Дополнительная литература:

1. Демьяненко, Н.Ю. Информационно-психологические воздействия в откр "Воронежский государственный технический университет", 2008. - 1 файл. - 30-00.
2. Остапенко Г.А. Информационные операции [Электронный ресурс] : учеб. - 30-00.
3. Остапенко, О.А. Опасность, ущербы и риски систем : Учеб. пособие / О.

8.2 Переченьинформационныхтехнологий,используемыхприосуществлени »,современныхпрофессиональныхбазданныхиинформационныхсправочныхс ист

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,НЕОБХОДИМАЯДЛЯОСУ ЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

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

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВ ОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Информационныеоперацииииатакираспределенныхком пьютерныхсистемах»читаютсялекции,проводятсялабораторныеработы,выпол няетсякурсовойпроект.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяна иболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражени явучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Методикавыполнениякурсовогопроектаизложенавучебно-методическомпособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременноивустановленныесроки.

Контрольусвоенияматериаладисциплиныпроизводитсяпроверкойкурсовогопроекта,защитойкурсовогопроекта.

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.

Лабораторнаяработа	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.
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, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.