МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ / А.Г. Остапенко /

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

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.1.Целидисциплины

Изучение подходов к определению информационного противоборства в мульт

1.2.Задачиосвоениядисциплины

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

Дисциплина«Информационноепротивоборствовмультисетевомпространстве»о

Процессизучениядисциплины«Информационноепротивоборствовмультисетево
ПК-12-способностьюпроводитьинструментальныймониторингзащищенностико
ПК-15-способностьюразрабатыватьпредложенияпосовершенствованиюсистем
ПСК-3.1-способностьюиспользоватьсовременныекритериииистандартыдляанал
ПСК-3.4-способностьюорганизовыватьзащитуинформациивраспределенныхко

Компетенция
ПК-12
ПК-15
ПСК-3.1
ПСК-3.4

Общаятрудоемкостьдисциплины«Информационноепротивоборствовмультисет
Распределениетрудоемкостидисциплиныповидамзанятий
очнаяформаобучения

Видыучебнойраб
Аудиторныезанятия (всего)
В томчисле:
Лекции
Практическиезанятия (ПЗ)
Самостоятельнаяработа
Видыпромежуточнойаттестации - зачет
Общая трудоемкость: академические часы зач.ед.

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидам

№ п/п	Наименованиетемы
1	СТРАТЕГИЯ ОБЕСЦЕНИВАНИЯ И ВЗВЕШЕННЫЕ СЕТИ на примере НЕФТЯНОЙ ОТРАСЛ
2	Моделирование сетевой атаки на нефтяную отрасль
3	Управление валютным курсом в условиях атак на нефтяную сеть
4	СТРАТЕГИЯ УСТРАНЕНИЯ И ВЗВЕШЕННЫЕ БЕСПРОВОДНЫЕ ИНФОРМАЦИОННЫЕ СЕТИ
5	Структурно-функциональная специфика блокирования элементов атакуемой беспроводной сети
6	2.3 Риск-анализ блокирования элементов беспроводной сети

5.2Перечьлабораторныхработ
Непредусмотреноучебнымпланом

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыпол

7.ОЦЕНОЧНЫЕМА

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличны

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяп
«аттестован»;
«неаттестован».

Компе-тенция	Результатыобучения,характеризу сформированностькомпетенц
ПК-12	знать: – принципы работы элементов и функциональных узлов компь 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 расчётов
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

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв8семестредляочнойф
«зачтено»

«незачтено»

Компе- тенция	Результатыобучения,характеризу сформированностькомпетенц
ПК-12	знать: – принципы работы элементов и функциональных узлов компь 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 расчётов
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 а защищенности КС

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияи

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, предуп
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
4) К основным принципам обеспечения информационной безопасности относи

+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

5) К основным функциям системы безопасности можно отнести все перечисле
+ 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 относя
+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 сред

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

•
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

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

(минимум10вопросовдлятестированиясвариантамиответов)

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

(минимум10вопросовдлятестированиясвариантамиответов)

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

Укажитевопросыдлязачета

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

Непредусмотреноучебнымпланом

7.2.6.Методикавыставленияоценкиприпроведениипромежуточнойаттеста

(Например:Экзаменпроводитсяпотест-билетам,каждыйизкоторыхсодержит
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	Контролируемыеразделы
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 элем
5	Структурно-функциональная специфика блокирования элементов
6	Риск-анализ блокирования элементов беспроводной сети

7.3.Методическиематериалы,определяющиепроцедурыоцениванияознаний

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирова
ометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсист
яоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттеста

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсисте
оценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестац

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

1. Остапенко, А.Г. Обнаружение и нейтрализация вторжений в распределен "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 откры "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.

8.2Переченьинформационныхтехнологий,используемыхприосуществлени »,современныхпрофессиональныхбазданныхиинформационныхсправочныхсист

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

Специализированная лекционная аудитория, оснащенная оборудованием для л

10.МЕ

Подисциплине«Информационноепротивоборствовмультисетевомпространстве
Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсянаиболее
Практическиезанятиянаправленынаприобретениепрактическихнавыковрасчета

Видучебныхзанятий	
Лекция	Нап терм реко
Практическое занятие	Кон зада
Самостоятельнаяработа	Сам - ра - вы - ра

	- уч - по
Подготовка к промежуточнойаттестации	Гот пер