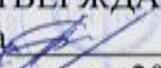


**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

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 Безопасность распределенных 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


/ 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 мультисетевом пространстве

1.2.Задачiosoвoениядисциплины

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

Дисциплина«Информационноепротивоборствовмультисетевомпространстве»о

Процессизучениядисциплины«Информационноепротивоборствовмультисетевомпространстве»о

ПК-12-способностьюпроводитьинструментальныймониторингзащищенностикомпьютерных

ПК-15-способностьюразрабатыватьпредложенияпосовершенствованиюсистеминформационной

ПСК-3.1-способностьюиспользоватьсовременныекритерииистандартыдляанализаинформационной

ПСК-3.4-способностьюорганизовыватьзащитуинформациивраспределенныхкомпьютерных

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

Общая трудоемкость дисциплины «Информационное противоборство в мультисетевых средах»
 Распределение трудоемкости дисциплины по видам занятий
очная форма обучения

Виды учебной работы
Аудиторные занятия (всего)
В том числе:
Лекции
Практические занятия (ПЗ)
Самостоятельная работа
Виды промежуточной аттестации - зачет
Общая трудоемкость:
академические часы
зач.ед.

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

№ п/п	Наименование темы
1	СТРАТЕГИЯ ОБЕСЦЕНИВАНИЯ И ВЗВЕШЕННЫЕ СЕТИ на примере НЕФТЯНОЙ ОТРАСЛИ
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

5.2 Перечень лабораторных работ Непредусмотрено учебным планом

В соответствии с учебным планом освоение дисциплины не предусматривает выполнения

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по

«аттестован»;

«неаттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-12	знать: – принципы работы элементов и функциональных узлов компьютерных систем в условиях информационного противоборства; уметь - проводить анализ качества показателей компьютерных систем владеть - навыками анализа основных характеристик и использования компьютерных систем в экспериментальном исследовании компьютерных систем.
ПК-15	знать - основные понятия и последовательность этапов решения задач, необходимых для совершенствования системы управления компьютерной системой; уметь - определить математический аппарат, необходимый для решения задач управления в рамках динамической системы управления без обратной связи в условиях информационного противоборства в мультисетевом пространстве; владеть - методиками построения линейных оптимальных систем управления компьютерной системы и их реализациями в современных информационных системах инженерных и научных расчётов
ПСК-3.1	знать - современные критерии оценки риска и стандарты для анализа безопасности распределенных компьютерных систем с рисками уметь - применять на практике подходы к аналитическому оцениванию нерегулярности распределения ущербов и их динамики
ПСК-3.4	знать - способы организации защиты информации в компьютерных системах противоборства в мультисетевом пространстве уметь - проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных систем владеть - инструментальными средствами проведения мониторинга и анализа защищенности КС

7.1.2 Этап промежуточного контроля знаний

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

«зачтено»

«незачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-12	знать: – принципы работы элементов и функциональных узлов компьютерных систем в условиях информационного противоборства; уметь - проводить анализ качества показателей компьютерных систем владеть - навыками анализа основных характеристик и использования компьютерных систем в экспериментальном исследовании компьютерных систем.
ПК-15	знать -основные понятия и последовательность этапов решения задач, необходимых для совершенствования системы управления компьютерной системы; уметь - определить математический аппарат, необходимый для решения задач управления в рамках динамической системы управления без обратной связи в условиях информационного противоборства в мультисетевом пространстве владеть - методиками построения линейных оптимальных систем управления компьютерной системы и их реализациями в современных информационных системах инженерных и научных расчётов
ПСК-3.1	знать - современные критерии оценки риска и стандарты для анализа безопасности распределенных компьютерных систем с учетом рисков уметь - применять на практике подходы к аналитическому оцениванию рисков нерегулярности распределения ущербов и их динамики
ПСК-3.4	знать - способы организации защиты информации в компьютерных системах в условиях информационного противоборства в мультисетевом пространстве уметь - проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных систем владеть -инструментальными средствами проведения мониторинга и аудита защищенности КС

7.2 Примерный перечень оценочных средств (типовые контрольные задания и тесты)

7.2.1 Примерный перечень заданий для подготовки к тестированию

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 и устранение:

- + несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

4) К основным принципам обеспечения информационной безопасности относятся:

- + 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-компания
- 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 деятельности:

- 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 сред

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 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

7.2.2 Примерный перечень заданий для решения стандартных задач
 (минимум 10 вопросов для тестирования с вариантами ответов)

7.2.3 Примерный перечень заданий для решения прикладных задач
 (минимум 10 вопросов для тестирования с вариантами ответов)

7.2.4 Примерный перечень вопросов для подготовки к зачету
 Укажите вопросы для зачета

7.2.5 Примерный перечень заданий для решения прикладных задач
 Непредусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации
 (Например: Экзамен проводится по тест-билетам, каждый из которых содержит определенное 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.)

7.2.7 Паспорт оценочных материалов

№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 элементов
5	Структурно-функциональная специфика блокирования элементов
6	Риск-анализ блокирования элементов беспроводной сети

7.3. Методические материалы, определяющие процедуры оценивания знаний

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо по методике выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо по методике выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо по методике выставления оценки при проведении промежуточной аттестации.

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Остапенко, А.Г. Обнаружение и нейтрализация вторжений в распределенных системах. Воронежский государственный технический университет, 2013. - 1 файл. - 30-00.
2. Остапенко О.А. Риски систем: Оценка и управление [Электронный ресурс]. Воронежский государственный технический университет, 2006. - 1 файл. - 30-00.
3. Кушнир, А.Э. Рефлексивные игры в информационном пространстве социальных сетей. Воронежский государственный технический университет, 2008. - 1 файл. - 30-00.

Дополнительная литература:

1. Демьяненко, Н.Ю. Информационно-психологические воздействия в открытых системах. Воронежский государственный технический университет, 2008. - 1 файл. - 30-00.
2. Остапенко Г.А. Информационные операции [Электронный ресурс] : учеб. пособие. - 30-00.
3. Остапенко, О.А. Опасность, ущербы и риски систем : Учеб. пособие / О.А. Остапенко. - Воронеж : ВГТУ, 2013. - 1 файл. - 30-00.

8.2 Перечень информационных технологий, используемых при осуществлении учебной деятельности, и 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/> (ЭБС IPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных занятий

10. МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Под дисциплину «Информационное противоборство в мультисетевом пространстве» разработаны методические материалы, включающие лекции, практические занятия, самостоятельную работу.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее сложные теоретические вопросы.

Практические занятия направлены на приобретение практических навыков расчета и анализа систем.

Вид учебных занятий	
Лекция	Направление
Практическое занятие	Курсовое задание
Самостоятельная работа	Самостоятельная работа - работа - выполнение - работа

	- уч - по
Подготовка к промежуточной аттестации	Гот пер