МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт физики

подписано электронно-цифровой подписью

Программа дисциплины

Физические основы защиты информации М2.Б.5

Направление подготовки: 011800.68 - Радиофизика
Профиль подготовки: Электромагнитные волны в средах
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Иванов К.В.

Рецензент(ы):

Акчурин А.Д.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Акчурин А. Д.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института физики:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 620214

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) ассистент, к.н. Иванов К.В. Кафедра радиоастрономии Отделение радиофизики и информационных систем , KVIvanov@kpfu.ru

1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) М2.Б.5. " Физические основы защиты информации " является получение теоретических знаний о функционировании современных средств защиты информации и практических навыков администрирования этих средств.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " М2.Б.5 Профессиональный" основной образовательной программы 011800.68 Радиофизика и относится к базовой (общепрофессиональной) части. Осваивается на 1 курсе, 2 семестр.

Дисциплина М2.Б.5. " Физические основы защиты информации " входит в цикл профессиональных дисциплин.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-1 (профессиональные компетенции)	способностью к свободному владению знаниями фундаментальных разделов физики и радиофизики, необходимыми для решения научно-исследовательских задач (в соответствии со своим профилем подготовки)
ПК-2 (профессиональные компетенции)	способностью к свободному владению профессионально-профильными знаниями в области информационных технологий, использованию современных компьютерных сетей, программных продуктов и ресурсов Интернет для решения задач профессиональной деятельности, в том числе находящихся за пределами профильной подготовки
ПК-5 (профессиональные компетенции)	способностью применять на практике навыки составления и оформления научно-технической документации, научных отчетов, обзоров, докладов и статей (в соответствии с профилем подготовки)
ПК-8 (профессиональные компетенции)	способностью составлять обзоры перспективных направлений научно-инновационных исследований, готовностью к написанию и оформлению патентов в соответствии с правилами

В результате освоения дисциплины студент:

1. должен знать:

принципы работы и организацию современных средств защиты информации;
функции и задачи, стоящие перед администраторами безопасности

2. должен уметь:

Администрировать средства защиты информации, встроенные в современные операционные системы, обеспечивающие дополнительный функционал для средств защиты СВТ, а также сетевые средства защиты информации.

3. должен владеть:

Навыками аргументированного выбора механизмов защиты информации, используемых при построении системы защиты информации Автоматизированных систем..

4. должен демонстрировать способность и готовность:

применять полученные знания на практике

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет во 2 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем.	2		2	1	0	
2.	Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.	2		2	3	0	
3.	Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.	2		3	3	0	
4.	Тема 4. Построение подсистемы антивирусной защиты.	2		2	3	0	
5.	Тема 5. Использование добавочных средств защиты.	2		2	2	0	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
6.	Тема 6. Построение системы межсетевого экранирования.	2		3	2	0	
7.	Тема 7. Средства защиты информации. активного сетевого оборудования.	2		2	2	0	
.	Тема . Итоговая форма контроля	2		0	0	0	зачет
	Итого			16	16	0	

4.2 Содержание дисциплины

Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем.

лекционное занятие (2 часа(ов)):

Техническое проектирование и реализация систем защиты корпоративных систем. Жизненный цикл корпоративный системы. Обзор подходов к созданию защищённых автоматизированных систем (АС). Проблемы проектирования и реализации защищенных АС. Синтез АС и его этапы.

практическое занятие (1 часа(ов)):

Подготовка технического проекта и выбор нормативных документов для реализации системы защиты информации предприятия.

Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.

лекционное занятие (2 часа(ов)):

Операционная система (ОС) Linux и её подсистема безопасности. Методика и практика использования систем на базе Linux. Возможности комплекса средств защиты (КСЗ) ОС. Подсистема разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема.

практическое занятие (3 часа(ов)):

Установка и настройка ОС RedHat, изучение возможностей подсистемы разграничения доступа, настройка подсистемы регистрации и учета, подсистемы обеспечения целостности.

Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.

лекционное занятие (3 часа(ов)):

Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности. Методика и практика использования технологий Microsoft. Возможности комплекса средств защиты (КСЗ) ОС. Подсистема разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема. Интерфейс администратора безопасности

практическое занятие (3 часа(ов)):

Установка и настройка ОС Windows 2008 Server, изучение возможностей подсистемы разграничения доступа, настройка подсистемы регистрации и учета, подсистемы обеспечения целостности. Работа с интерфейсом администратора безопасности.

Тема 4. Построение подсистемы антивирусной защиты.

лекционное занятие (2 часа(ов)):

Построение подсистемы антивирусной защиты. Классификация вредоносного программного обеспечения (ПО). Обзор существующих методов и средств антивирусной защиты. Стратегии антивирусной защиты.

практическое занятие (3 часа(ов)):

Установка и настройка антивирусной защиты на основе Kaspersky Business Space Security.

Тема 5. Использование добавочных средств защиты.

лекционное занятие (2 часа(ов)):

Использование добавочных средств защиты. Средства резервного копирования информации. Виртуальные частные сети.

практическое занятие (2 часа(ов)):

Настройка средств резервного копирование. Моделирование виртуальных частных сетей на предприятии.

Тема 6. Построение системы межсетевого экранирования.

лекционное занятие (3 часа(ов)):

Построение системы межсетевого экранирования. Межсетевые экраны на безе ОС Windows и Linux. Создание системы обнаружения вторжений.

практическое занятие (2 часа(ов)):

Установка и настройка межсетевого экрана iptables. Реализация системы обнаружения вторжений на примере Suricata IDS.

Тема 7. Средства защиты информации. активного сетевого оборудования.

лекционное занятие (2 часа(ов)):

Средства защиты информации. активного сетевого оборудования. Списки контроля доступа. Виртуальные локальные сети. Использование инструментальных средств анализа защищённости.

практическое занятие (2 часа(ов)):

Использование сканера уязвимостей Nessus для анализа защищенности предприятия.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем.	2		Подготовка и написание отчета.	3	Отчёт
2.	Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.	2		Подготовка и написание отчета.	6	Отчёт
3.	Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.	2		Подготовка и написание отчета.	6	Отчёт
4.	Тема 4. Построение подсистемы антивирусной защиты.	2		Подготовка и написание отчета.	6	Отчёт

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
5.	Тема 5. Использование добавочных средств защиты.	2		Подготовка и написание отчета.	7	Отчёт
6.	Тема 6. Построение системы межсетевого экранирования.	2		Подготовка и написание отчета.	7	Отчёт
7.	Тема 7. Средства защиты информации. активного сетевого оборудования.	2		Подготовка и написание отчета.	5	Отчёт
	Итого				40	

5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций читается на основе мультимедийных технологий, практические занятия проводятся в классе многопользовательского терминального доступа.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем.

Отчёт, примерные вопросы:

Отчет и технический проект с выбранным набором нормативных документов для реализации системы защиты информации предприятия.

Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.

Отчёт, примерные вопросы:

Отчет об установке и настройке ОС RedHat, настройки подсистемы разграничения доступа, подсистемы регистрации и учета, подсистемы обеспечения целостности.

Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.

Отчёт, примерные вопросы:

Отчет об установке и настройке ОС Windows 2008 Server, изучении возможностей подсистемы разграничения доступа, настройке подсистемы регистрации и учета, подсистемы обеспечения целостности. Описание элементов интерфейса администратора безопасности использованных в ходе работы.

Тема 4. Построение подсистемы антивирусной защиты.

Отчёт, примерные вопросы:

Отчет об установке и настройке антивирусной защиты на основе Kaspersky Business Space Security.

Тема 5. Использование добавочных средств защиты.

Отчёт, примерные вопросы:

Отчет о настройке средств резервного копирования. Моделирование виртуальных частных сетей на предприятии.

Тема 6. Построение системы межсетевого экранирования.

Отчёт, примерные вопросы:

Отчет об установке и настройке межсетевого экрана iptables и реализации системы обнаружения вторжений на примере Suricata IDS.

Тема 7. Средства защиты информации. активного сетевого оборудования.

Отчёт, примерные вопросы:

Отчет сканера уязвимостей Nessus и подготовка рекомендаций для анализа защищенности предприятия на основе выявленных нарушений.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ (СРС) включает следующие виды работ:

- изучение теоретического лекционного материала;
- проработка теоретического материала (конспекты лекций, основная и дополнительная литература, использование ресурсов интернета);
- выполнение работ;
- подготовка к сдаче зачета по изучаемой дисциплине.

Разработанный блок вопросов для компьютерной системы тестирования TCExam.

Вопросы к зачету

1. Подсистема управления доступом. Особенности реализации в различных ОС
2. Подсистема регистрации и учёта событий. Особенности реализации в различных ОС
3. Криптографическая подсистема. Особенности реализации в различных ОС
4. Подсистема обеспечения целостности. Особенности реализации в различных ОС
5. Построение подсистемы антивирусной защиты
6. Межсетевые экраны. определение, назначение, классификации.
7. Архитектура систем активного аудита
8. Обзор инструментальных средств анализа защищённости АС
9. Средства защиты информации. активного сетевого оборудования

7.1. Основная литература:

1. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: http://znanium.com/bookread.php?book=474838

2. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. http://znanium.com/bookread.php?book=432654

3. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. http://znanium.com/bookread.php?book=476047

4. Партыка Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. http://znanium.com/bookrea,d.php?book=420047

5.Молдовян Н. А. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - СПб.: БХВ-Петербург, 2010. - 293 с. - (Учебное пособие) http://znanium.com/bookread.php?book=351283

7.2. Дополнительная литература:

1.Чмора А. Л.. Современная прикладная криптография: Учеб. пособие : Гелиос АРВ, 2001.256с.:

2. Лопатин В. Н. Информационная безопасность России: СПб.: Фонд "Университет", 2000. 426с..

3. Бабаш, А. В. Криптография М.: СОЛОН-Р, 2002.?509с.

4. Левин М. Криптография: Руководство пользователя М.: Познавательная книга плюс, 2001.319с.

5. Столлингс В. Основы защиты сетей. Приложения и стандарты ?М.: Издат. Дом "Вильямс", 2002.429с

6. Столлингс, Вильям. Криптография и защита сетей. Принципы и практика ?М.: Издат. Дом "Вильямс", 2001.669с.:

7.3. Интернет-ресурсы:

Всё об инфрмационных систмах персональных данных - http://www.ispdn.ru/

Искусство управления информационной безопасностью - http://iso27000.ru/

КСайт федеральной службы по техническому и экспортному контролю - http://fstec.ru/

Центр безопасности Microsoft - http://www.microsoft.com/ru-ru/security/default.aspx

Эшелон. Комплексная безопасность - http://s3r.ru/

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Физические основы защиты информации" предполагает использование следующего материально-технического обеспечения:

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Компьютерный класс, позволяющий развёртывать на каждой ЭВМ не менее 2 виртуальных машин.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 011800.68 "Радиофизика" и магистерской программе Электромагнитные волны в средах .

Автор(ы):
Иванов К.В. _____
"__" _____ 201 __ г.

Рецензент(ы):
Акчурин А.Д. _____
"__" _____ 201 __ г.