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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.

подписано электронно-цифровой подписью

Программа дисциплины

Программно-аппаратные средства защиты информации Б3.Б.3

Направление подготовки: 090900.62 - Информационная безопасность
Профиль подготовки: Информационная безопасность автоматизированных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Иванов К.В.

Рецензент(ы):

Корчагин П.А.

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 643014

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) Б3.Б3. "Программно-аппаратные средства информационной безопасности " 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 " Б3.Б.3 Профессиональный" основной образовательной программы 090900.62 Информационная безопасность и относится к базовой (общепрофессиональной) части. Осваивается на 4 курсе, 7 семестр.

Дисциплина Б3.Б3. " Программно-аппаратные средства информационной безопасности " входит в цикл дисциплин "Профессиональный".

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-11 (общекультурные компетенции)	способен уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия
ОК-13 (общекультурные компетенции)	способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны
ОК-14 (общекультурные компетенции)	способен применять основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий, технику безопасности на производстве
ПК-1 (профессиональные компетенции)	способен использовать нормативные правовые документы в профессиональной деятельности
ПК-18 (профессиональные компетенции)	способен анализировать и выбирать методы и средства обеспечения информационной безопасности

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 программно-технические способы и средства для обеспечения информационной безопасности объекта.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 5 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 7 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.	7	1	2	0	0	устный опрос
2.	Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.	7	2	8	0	8	контрольная работа
3.	Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.	7	7	8	0	8	устный опрос контрольная работа
4.	Тема 4. Построение подсистемы антивирусной защиты.	7	14	2	0	2	устный опрос
5.	Тема 5. Использование добавочных средств защиты.	7	15	2	0	2	устный опрос

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.	7	16	4	0	6	устный опрос
7.	Тема 7. Средства защиты информации активного сетевого оборудования.	7	18	10	0	10	устный опрос
.	Тема . Итоговая форма контроля	7		0	0	0	экзамен
	Итого			36	0	36	

4.2 Содержание дисциплины

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

лекционное занятие (2 часа(ов)):

- Жизненный цикл защищённой корпоративной АС - Функции администратора безопасности и инструменты их реализации - Средства борьбы с несанкционированным доступом (НСД) к информационным ресурсам. - Системы комплексного администрирования безопасности: система комплексного администрирования безопасности (СКАД).

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

лекционное занятие (8 часа(ов)):

- Возможности комплекса средств защиты (КСЗ) ОС - Подсистема разграничения доступа - Подсистема регистрации и учёта - Подсистема обеспечения целостности - Криптографическая подсистема - Интерфейс администратора безопасности

лабораторная работа (8 часа(ов)):

Упражнение 1. Управление учетными записями пользователей и создание групп Упражнение 2. Настройка подсистемы идентификации и аутентификации пользователей Упражнение 3. Установка прав разграничения доступа к файлам Упражнение 4. Настройка подсистемы регистрации и учёта событий

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

лекционное занятие (8 часа(ов)):

- Возможности КСЗ ОС семейства Windows - Подсистема разграничения доступа - Подсистема регистрации и учёта - Подсистема обеспечения целостности - Криптографическая подсистема - Интерфейс администратора безопасности

лабораторная работа (8 часа(ов)):

Упражнение 1. Управление учетными записями пользователей и создание групп Упражнение 2. Управление разрешениями в файловой системе NTFS Упражнение 3. Управление локальными политиками безопасности Упражнение 4. Создание и изменение шаблона политики безопасности Упражнение 5. Анализ шаблона политики безопасности Упражнение 6. Настройка подсистемы регистрации и учёта событий

Тема 4. Построение подсистемы антивирусной защиты.

лекционное занятие (2 часа(ов)):

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

лабораторная работа (2 часа(ов)):

Установка и настройка антивирусного пакета корпоративной версии

Тема 5. Использование добавочных средств защиты.

лекционное занятие (2 часа(ов)):

Стратегии резервного копирования. Классификация решений VPN

лабораторная работа (2 часа(ов)):

Построение системы резервного копирования в ОС семейства WIndows Установка и настройка ПО VipNet

Тема 6. Построение системы межсетевого экранирования.

лекционное занятие (4 часа(ов)):

Компоненты корпоративной сети, определяющие уровень безопасности Межсетевое экранирование .Обзор и классификация межсетевых экранов.Построение системы обнаружения вторжений Проблема эксплуатации защищённых АС, администрирование безопасности информации

лабораторная работа (6 часа(ов)):

Использование инструментальных средств анализа защищённости. Установка и использование сканера Nessus.

Тема 7. Средства защиты информации активного сетевого оборудования.

лекционное занятие (10 часа(ов)):

Компоненты корпоративной сети, определяющие уровень безопасности Межсетевое экранирование .Обзор и классификация межсетевых экранов.Построение системы обнаружения вторжений Проблема эксплуатации защищённых АС, администрирование безопасности информации

лабораторная работа (10 часа(ов)):

Упражнение №1. Обзор средств разграничения доступа на активном оборудовании
Упражнение №2 Использование средств разграничения доступа на нескольких коммутаторах
Упражнение №3. Создание и удаление виртуальных сетей на коммутаторе Catalyst 2950

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.	7	1	подготовка к устному опросу	2	устный опрос
2.	Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.	7	2	подготовка к контрольной работе	16	контрольная работа
3.	Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.	7	7	подготовка к контрольной работе	16	контрольная работа
4.	Тема 4. Построение подсистемы антивирусной защиты.	7	14	подготовка к устному опросу	2	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
5.	Тема 5. Использование добавочных средств защиты.	7	15	подготовка к устному опросу	2	устный опрос
6.	Тема 6. Построение системы межсетевого экранирования.	7	16	подготовка к устному опросу	14	устный опрос
7.	Тема 7. Средства защиты информации активного сетевого оборудования.	7	18	подготовка к устному опросу	20	устный опрос
	Итого				72	

5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций читается на основе мультимедийных технологий,.

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.

устный опрос , примерные вопросы:

Стадии создания АС, стадии создания ПО. Особенности написания ТЗ.

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

контрольная работа , примерные вопросы:

- Возможности комплекса средств защиты (КСЗ) ОС - Подсистема разграничения доступа - Подсистема регистрации и учёта - Подсистема обеспечения целостности - Криптографическая подсистема - Интерфейс администратора безопасности Инсталляция ОС Linux. Настройка подсистемы разграничения доступа. Настройка подсистемы регистрации и учёта. Настройка подсистемы обеспечения целостности. Настройка и использование криптографической подсистемы. Системы LIDS и RSBAC.

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

контрольная работа , примерные вопросы:

Инсталляция ОС Windows. Настройка подсистемы разграничения доступа. Настройка подсистемы регистрации и учёта. Настройка подсистемы обеспечения целостности. Настройка и использование криптографической подсистемы. Интерфейс администратора безопасности. Передача административного контроля. Использование оснасток. Создание антивирусной подсистемы. Построение системы управления обновлениями - Возможности КСЗ ОС семейства Windows - Подсистема разграничения доступа - Подсистема регистрации и учёта - Подсистема обеспечения целостности - Криптографическая подсистема

Тема 4. Построение подсистемы антивирусной защиты.

устный опрос , примерные вопросы:

Стратегии антивирусной защиты. Классификация вредоносного ПО

Тема 5. Использование добавочных средств защиты.

устный опрос , примерные вопросы:

Классификация VPN. Определение SSL.

Тема 6. Построение системы межсетевого экранирования.

устный опрос , примерные вопросы:

Классификация и определение межсетевых экранов

Тема 7. Средства защиты информации активного сетевого оборудования.

устный опрос , примерные вопросы:

Виды сетевого оборудования и механизмы его защиты

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Разработанный блок вопросов для компьютерной системы тестирования TCExam.

Вопросы к экзамену

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:

Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. Режим доступа: http://znanium.com/bookread.php?book=405000

Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5. Режим доступа: http://znanium.com/bookread.php?book=423927

Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с.: http://znanium.com/bookread.php?book=169345

7.2. Дополнительная литература:

Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4

- http://znanium.com/catalog.php?bookinfo=402686

Аверченков В И Рытов М. Ю. Аверченков, В. И. Организационная защита информации [электронный ресурс] : учеб.пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - 3-е изд., стереотип. - М. : ФЛИНТА, 2011. - 184 с. :http://znanium.com/bookread.php?book=453862

7.3. Интернет-ресурсы:

Аверченков В И Рытов М. Ю. Аверченков, В. И. Организационная защита информации [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов. 3-е изд., стереотип. М. : ФЛИНТА, 2011. - http://znanium.com/bookread.php?book=453862

Бабаш А. В. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - http://znanium.com/bookread.php?book=405000

Кузнецов И. Н. Кузнецов, И. Н. Бизнес-безопасность [Электронный ресурс] / И. Н. Кузнецов. - 3-е изд. - М.: Дашков и К, 2013. - http://znanium.com/bookread.php?book=430343

Партыка Т. Л. Попов И. И. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2008. - http://znanium.com/catalog.php?bookinfo=167284

Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - http://znanium.com/bookread.php?book=169345

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Программно-аппаратные средства защиты информации" предполагает использование следующего материально-технического обеспечения:

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

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 090900.62 "Информационная безопасность" и профилю подготовки Информационная безопасность автоматизированных систем .

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

Рецензент(ы):
Корчагин П.А. _____
"__" _____ 201 __ г.