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. Таюрский Д.А.

_____ _____20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Программно-аппаратные средства информационной безопасности Б1.В.ДВ.15

Направление подготовки: 03.03.03 - Радиофизика
Профиль подготовки: Специальные радиотехнические системы
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Акчурин А.Д. , Иванов К.В. , Иванов Константин Васильевич

Рецензент(ы):

Шерстюков О.Н.

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 635918

Казань
2018

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Акчурин А.Д. Кафедра радиоастрономии Отделение радиофизики и информационных систем , Adel.Akchurin@kpfu.ru ; Иванов К.В. , KVIvanov@kpfu.ru ; Иванов Константин Васильевич

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 " Б1.В.ДВ.15 Дисциплины (модули)" основной образовательной программы 03.03.03 Радиофизика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 8 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
ОПК-4 (профессиональные компетенции)	способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
ПК-1 (профессиональные компетенции)	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-2 (профессиональные компетенции)	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-3 (профессиональные компетенции)	способностью администрировать подсистемы информационной безопасности объекта защиты

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 4 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 8 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.	8	1	4	0	4	Устный опрос
2.	Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.	8	2	6	0	8	Контрольная работа
3.	Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.	8	7	6	0	8	Устный опрос Контрольная работа
4.	Тема 4. Построение подсистемы антивирусной защиты.	8	14	4	0	6	Устный опрос
5.	Тема 5. Использование добавочных средств защиты.	8	15	6	0	6	Устный опрос
6.	Тема 6. Построение системы межсетевого экранирования.	8	16	4	0	8	Устный опрос
7.	Тема 7. Средства защиты информации активного сетевого оборудования.	8	18	6	0	10	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	
.	Тема . Итоговая форма контроля	8		0	0	0	Экзамен
	Итого			36	0	50	

4.2 Содержание дисциплины

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

лекционное занятие (4 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).

лабораторная работа (4 часа(ов)):

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

лекционное занятие (6 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 (6 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 (4 часа(ов)):

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

лабораторная работа (6 часа(ов)):

Установка и настройка антивирусного пакета корпоративной версии

Тема 5. Использование добавочных средств защиты.

лекционное занятие (6 часа(ов)):

Стратегии резервного копирования. Классификация решений VPN

лабораторная работа (6 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 (8 часа(ов)):

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

Тема 7. Средства защиты информации активного сетевого оборудования.

лекционное занятие (6 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.	8	1	подготовка к устному опросу	1	Устный опрос
2.	Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.	8	2	подготовка к контрольной работе	2	Контрольная работа
3.	Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.	8	7	подготовка к контрольной работе	2	Контрольная работа
4.	Тема 4. Построение подсистемы антивирусной защиты.	8	14	подготовка к устному опросу	2	Устный опрос
5.	Тема 5. Использование добавочных средств защиты.	8	15	подготовка к устному опросу	2	Устный опрос
6.	Тема 6. Построение системы межсетевого экранирования.	8	16	подготовка к устному опросу	2	Устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
7.	Тема 7. Средства защиты информации активного сетевого оборудования.	8	18	подготовка к устному опросу	2	Устный опрос
	Итого				13	

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:

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.

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

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

Контрольная работа , примерные вопросы:

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

Тема 4. Построение подсистемы антивирусной защиты.

Устный опрос , примерные вопросы:

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

Тема 5. Использование добавочных средств защиты.

Устный опрос , примерные вопросы:

Стратегии резервного копирования. Классификация решений VPN

Тема 6. Построение системы межсетевого экранирования.

Устный опрос , примерные вопросы:

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

Тема 7. Средства защиты информации активного сетевого оборудования.

Устный опрос , примерные вопросы:

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

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Вопросы к экзамену:

1. Построение подсистемы антивирусной защиты.
2. Межсетевые экраны. определение, назначение, классификации.
3. Обзор инструментальных средств анализа защищённости АС.
4. Средства защиты информации. активного сетевого оборудования.
5. Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации
6. Организационная поддержка мер защиты. Отраслевые стандарты
7. Пакет руководящих документов Гостехкомиссии России
8. ISO 15408. Единые критерии
9. Особенности ISO 15408 по сравнению с другими стандартами в области безопасности
10. Документы ФСТЭК России, разработанные на базе ISO 15408
11. Подсистема управления доступом
12. Подсистема обеспечения целостности
13. Подсистема регистрации и учёта событий
14. Криптографическая подсистема
15. КСЗ ОС семейства Windows. Подсистема управления доступом
16. КСЗ ОС семейства Windows. Подсистема обеспечения целостности
17. КСЗ ОС семейства Windows. Подсистема регистрации и учёта событий.
18. КСЗ ОС семейства Windows. Криптографическая подсистема
19. КСЗ ОС Linux. Подсистема управления доступом.
20. КСЗ ОС Linux. Подсистема обеспечения целостности
21. КСЗ ОС Linux. Подсистема регистрации и учёта событий.
22. КСЗ ОС Linux. Криптографическая подсистема.
23. Применение средств защиты в активном сетевом оборудовании, и при построении защищённых сетей.
24. Построение системы межсетевого экранирования .
25. Построение системы обнаружения вторжений.
26. Понятие сертификации. Основные участники сертификации.
27. Схемы сертификационных испытаний. Инспекционный контроль.
28. Порядок проведения сертификационных испытаний.

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 информационной безопасности" 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.

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 03.03.03 "Радиофизика" и профилю подготовки Специальные радиотехнические системы .

Автор(ы):
Акчурин А.Д. _____
Иванов К.В. _____
Иванов Константин Васильевич _____
"__" _____ 201 __ г.

Рецензент(ы):
Шерстюков О.Н. _____
"__" _____ 201 __ г.