МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____ "___" _____ 20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Программно-аппаратные средства защиты информации Б3.Б.3

Направление подготовки: 090900.62 - Информационная безопасность
Профиль подготовки: Математические и программные средства защиты информации
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Разинков Е.В.

Рецензент(ы):
Латыпов Р.Х.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 971515

Казань
2015

Содержание

Программу дисциплины разработал(а)(и) ассистент, к.н. Разинков Е.В. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Evgenij.Razinkov@kpfu.ru

1. Цели освоения дисциплины

Целями освоения данной учебной дисциплины являются:

1. Получить представление о существующих программно-аппаратных средствах защиты информационных систем.

2. Уметь устанавливать, конфигурировать и обслуживать программно-аппаратные средства защиты информационных систем.

3. Получить представление о функционировании программных и аппаратных средств защиты информационных систем.

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 3 курсе, 6 семестр.

Данная дисциплина входит в базовую часть профессионального цикла дисциплин. Изучается на 3 курсе в 6 семестре.

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)	способность к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства
ОК-12 (общекультурные компетенции)	способность критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков
ОК-8 (общекультурные компетенции)	способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления
ОК-9 (общекультурные компетенции)	способность логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссию
ПК-10 (профессиональные компетенции)	способность администрировать подсистемы информационной безопасности объекта
ПК-11 (профессиональные компетенции)	способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-5 (профессиональные компетенции)	способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации
ПК-6 (профессиональные компетенции)	способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов

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 и навыки в своей дальнейшей профессиональной деятельности.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 6 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. Защита						

информации в автоматизированных системах.

						домашнее
6		6	6	0		

задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Защита информации в ОС Linux.	6		6	6	0	домашнее задание
3.	Тема 3. Защита информации в ОС Windows.	6		6	6	0	домашнее задание
4.	Тема 4. Антивирусная защита.	6		6	6	0	контрольная работа домашнее задание
5.	Тема 5. Средства обеспечения целостности информации.	6		4	4	0	домашнее задание
6.	Тема 6. Сетевая безопасность.	6		4	4	0	домашнее задание
7.	Тема 7. Активное сетевое оборудование и защита информации.	6		4	4	0	контрольная работа домашнее задание
.	Тема . Итоговая форма контроля	7		0	0	0	зачет
	Итого			36	36	0	

4.2 Содержание дисциплины

Тема 1. Защита информации в автоматизированных системах.

лекционное занятие (6 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 (6 часа(ов)):

Сравнительный анализ подходов к созданию защищенных автоматизированных систем.

Тема 2. Защита информации в ОС Linux.

лекционное занятие (6 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 регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема.

практическое занятие (6 часа(ов)):

Контроль доступа в ОС Linux.

Тема 3. Защита информации в ОС Windows.

лекционное занятие (6 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 (6 часа(ов)):

Контроль доступа в ОС Windows.

Тема 4. Антивирусная защита.

лекционное занятие (6 часа(ов)):

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

практическое занятие (6 часа(ов)):

Применение средств антивирусной защиты.

Тема 5. Средства обеспечения целостности информации.

лекционное занятие (4 часа(ов)):

Целостность информации. Предотвращение нарушения целостности информации, обнаружение нарушения целостности информации, восстановление информации.

практическое занятие (4 часа(ов)):

Средства резервного копирования информации.

Тема 6. Сетевая безопасность.

лекционное занятие (4 часа(ов)):

Принципы построения системы межсетевого экранирования. Межсетевые экраны на базе ОС Windows и Linux. Виртуальные частные сети.

практическое занятие (4 часа(ов)):

Создание системы обнаружения вторжений.

Тема 7. Активное сетевое оборудование и защита информации.

лекционное занятие (4 часа(ов)):

Средства защиты информации в активном сетевом оборудовании. Списки контроля доступа. Виртуальные локальные сети.

практическое занятие (4 часа(ов)):

Использование инструментальных средств анализа защищённости.

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. Защита информации в автоматизированных системах.	6		подготовка домашнего задания	12	домашнее задание
2.	Тема 2. Защита информации в ОС Linux.	6		подготовка домашнего задания	12	домашнее задание
3.	Тема 3. Защита информации в ОС Windows.	6		подготовка домашнего задания	12	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
4.	Тема 4. Антивирусная защита.	6		подготовка домашнего задания	8	домашнее задание
				подготовка к контрольной работе	4	контрольная работа
5.	Тема 5. Средства обеспечения целостности информации.	6		подготовка домашнего задания	8	домашнее задание
6.	Тема 6. Сетевая безопасность.	6		подготовка домашнего задания	8	домашнее задание
7.	Тема 7. Активное сетевое оборудование и защита информации.	6		подготовка домашнего задания	6	домашнее задание
				подготовка к контрольной работе	2	контрольная работа
	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. Защита информации в автоматизированных системах.

домашнее задание , примерные вопросы:

Реализация программной системы парольной аутентификации.

Тема 2. Защита информации в ОС Linux.

домашнее задание , примерные вопросы:

Изучение символьных псевдоустройств ОС Linux /dev/random и /dev/urandom

Тема 3. Защита информации в ОС Windows.

домашнее задание , примерные вопросы:

Атака на переполнение буфера в ОС Windows.

Тема 4. Антивирусная защита.

домашнее задание , примерные вопросы:

Изучение средств обнаружения полиморфных вирусов.

контрольная работа , примерные вопросы:

Программная реализация простого антивируса на основе сигнатурного анализа.

Тема 5. Средства обеспечения целостности информации.

домашнее задание , примерные вопросы:

Реализация вычисления контрольной суммы CRC.

Тема 6. Сетевая безопасность.

домашнее задание , примерные вопросы:

Изучение принципов построения VPN.

Тема 7. Активное сетевое оборудование и защита информации.

домашнее задание , примерные вопросы:

Анализ уязвимостей активного сетевого оборудования.

контрольная работа , примерные вопросы:

Программная реализация системы контроля целостности.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

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. Контрольная сумма CRC.
6. Межсетевые экраны. Определение, назначение, классификация.
7. Архитектура систем активного аудита.
8. Обзор инструментальных средств анализа защищённости АС.
9. Средства защиты информации активного сетевого оборудования.
10. Генерация случайных чисел в ОС Linux.
11. Атака на переполнение буфера.
12. Принципы построения систем обнаружения вторжений.
13. Сигнатурный анализ как антивирусная техника.
14. Эвристические антивирусные техники.
15. Статические и динамические антивирусные техники.
16. Полиморфизм компьютерных вирусов.
17. Методы защиты от атаки на переполнение буфера.
18. Виртуальные частные сети.
19. Дискреционный контроль доступа.
20. Сравнительный анализ средств защиты информации различных операционных систем.

Типовой билет:

1. Дискреционный контроль доступа.
2. Атака на переполнение буфера.

7.1. Основная литература:

1. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для студ.высш.учеб.заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова.?М.: Академия, 2006.?336 с.

2. Столов Е.Л. Генераторы случайных чисел в системах компьютерной безопасности. - Казань, 2014, URL: http://shelly.kpfu.ru/e-ksu/docs/F833856100/FinalGen.pdf.

3. Червяков Н.И., Евдокимов А.А., Галушкин А.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. - - М.: Физматлит, 2012. - 280с.

http://e.lanbook.com/books/element.php?pl1_id=5300

4. 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. http://znanium.com/catalog.php?bookinfo=405000

5.Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. http://znanium.com/bookread.php?book=405313

7.2. Дополнительная литература:

1. Биктимиров, М. Р. Избранные главы компьютерной безопасности / М.Р. Биктимиров, А.Ю. Щербаков.?Казань: Изд-во КМО, 2004.?371 с.

2. Иванов, К. В. Марковские модели защиты автоматизированных систем управления специального назначения / К. В. Иванов, П. И. Тутубалин.?Казань: [Республиканский центр мониторинга качества образования], 2012.?213 с.

7.3. Интернет-ресурсы:

Википедия - http://ru.wikipedia.org

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет-портал по информационной безопасности - http://all-ib.ru/

Интернет-портал со статьями по алгоритмике и программированию - http://algolist.manual.ru/

Электронная библиотека по техническим наукам - http://techlibrary.ru

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 Математические и программные средства защиты информации .

Автор(ы):
Разинков Е.В. _____
"__" _____ 201 __ г.

Рецензент(ы):
Латыпов Р.Х. _____
"__" _____ 201 __ г.