

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.

_____ 20__ г.

Программа дисциплины

Физические основы защиты информации и информационная безопасность систем СД.ДС.Ф.6

Специальность: 010801.65 - Радиофизика и электроника

Специализация: Защита информации

Квалификация выпускника: РАДИОФИЗИК

Форма обучения: очное

Язык обучения: русский

Автор(ы):

Иванов К.В.

Рецензент(ы):

-

СОГЛАСОВАНО:

Заведующий(ая) кафедрой:

Протокол заседания кафедры No ____ от "____" _____ 201__ г

Учебно-методическая комиссия Института физики:

Протокол заседания УМК No ____ от "____" _____ 201__ г

Регистрационный No

Казань
2013

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

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) СД. ДС.Ф.6 "Физические основы защиты информации и информационная безопасность" является получение теоретических знаний о методах обеспечения информационной безопасности предприятия на основе использования современных средств защиты и инструментальных средств администрирования и практические навыки организации обеспечения защиты информации корпоративных информационных систем, формирования требований к проектируемым АС и ИСПДн и к комплексной системе защиты информации (СЗИ), построения защищенной информационной системы, формирования требований к обслуживанию комплексной СЗИ

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

Данная учебная дисциплина включена в раздел " СД.ДС.Ф.6 Специальные дисциплины (специализации)" основной образовательной программы 010801.65 Радиофизика и электроника и относится к федеральному компоненту. Осваивается на 4 курсе, 8 семестр.

Дисциплина СД.ДС.Ф.6. " Физические основы защиты информации и информационная безопасность " входит в цикл дисциплин "Дисциплины по выбору".

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

В результате освоения дисциплины формируются следующие компетенции:

В результате освоения дисциплины студент:

1. должен знать:

основные направления развития современных технологий защиты информации, лежащих в основе современных средств защиты информации автоматизированных систем;

2. должен уметь:

выдвигать требования к системам защиты информации ограниченного доступа;

3. должен владеть:

навыками формирования политики безопасности организации.

Демонстрировать способность и готовность

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет зачетных(ые) единиц(ы) 60 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. Введение в информационную безопасность. Основные термины и определения. □ Информация и её свойства □ Автоматизированная система и её ресурсы □ Доступ и его виды □ Обзор проблемных областей информационной безопасности.	8		0	0	0	
2.	Тема 2. Подсистемы обеспечения информационной безопасности □ Криптографическая подсистема □ Подсистема управления доступом □ Подсистема обеспечения целостности □ Подсистема регистрации и учёта событий □	8		0	0	0	
3.	Тема 3. Уязвимости, угрозы, атаки информационных систем и методы борьбы с ними. □ Угрозы безопасности информации в АС □ Классификация угроз и уязвимостей □ Анализ угроз АС □ Типовые угрозы безопасности □ Фазы атаки Сетевые атаки и способы защиты от них □	8		0	0	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	
4.	Тема 4. Организационно-правовая поддержка деятельности администратора безопасности. □ Обзор законов и подзаконных актов РФ, связанных с обеспечением информационной безопасности □ Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации □ Пакет руководящих документов Гостехкомиссии России □ Специальные требования и рекомендации по технической защите конфиденциальной информации Особенности защиты персональных данных	8		0	0	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	
5.	Тема 5. Международные стандарты информационной безопасности: ИСО/МЭК 15408-2002, ISO17799 □ ISO 15408. Общие критерии □ Профили защиты □ Функциональные требования □ Требования доверия □ Особенности ISO 15408 по сравнению с другими стандартами в области безопасности Стандарт ISO 17799 и его структура. Анализ рисков	8		0	0	0	
6.	Тема 6. Политика информационной безопасности организации. □ Определения политики информационной безопасности □ Концепция информационной безопасности организации □ Локальные политики информационной безопасности и должностные инструкции □ Аварийный план	8		0	0	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	
7.	Тема 7. Обзор существующих средств защиты информации. Аттестация объектов информатизации. Проблема эксплуатации защищённых АС, администрирование безопасности информации АС. Виды деятельности, функции и задачи администрирования. Виды деятельности администратора КСЗ. Функции и задачи администрирования.	8		0	0	0	
	Тема . Итоговая форма контроля	8		0	0	0	экзамен
	Итого			0	0	0	

4.2 Содержание дисциплины

Тема 1. Введение в информационную безопасность. Основные термины и определения.
 □ Информация и её свойства □ Автоматизированная система и её ресурсы □ Доступ и его виды
 Обзор проблемных областей информационной безопасности.

Тема 2. Подсистемы обеспечения информационной безопасности □ Криптографическая подсистема □ Подсистема управления доступом □ Подсистема обеспечения целостности □ Подсистема регистрации и учёта событий

Тема 3. Уязвимости, угрозы, атаки информационных систем и методы борьбы с ними. □ Угрозы безопасности информации в АС □ Классификация угроз и уязвимостей □ Анализ угроз АС □ Типовые угрозы безопасности □ Фазы атаки Сетевые атаки и способы защиты от них

Тема 4. Организационно-правовая поддержка деятельности администратора безопасности. □ Обзор законов и подзаконных актов РФ, связанных с обеспечением информационной безопасности □ Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации □ Пакет руководящих документов Гостехкомиссии России □ Специальные требования и рекомендации по технической защите конфиденциальной информации Особенности защиты персональных данных

Тема 5. Международные стандарты информационной безопасности: ИСО/МЭК 15408-2002, ISO17799 □ ISO 15408. Общие критерии □ Профили защиты □ Функциональные требования □ Требования доверия □ Особенности ISO 15408 по сравнению с другими стандартами в области безопасности Стандарт ISO 17799 и его структура. Анализ рисков

Тема 6. Политика информационной безопасности организации. □ Определения политики информационной безопасности □ Концепция информационной безопасности организации □ Локальные политики информационной безопасности и должностные инструкции □ Аварийный план

Тема 7. Обзор существующих средств защиты информации. Аттестация объектов информатизации. Проблема эксплуатации защищённых АС, администрирование безопасности информации АС. Виды деятельности, функции и задачи администрирования. Виды деятельности администратора КСЗ. Функции и задачи администрирования.

5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций читается на основе мультимедийных технологий, практические занятия проводятся в лаборатории, оснащенной современными учебными комплексами и измерительной аппаратурой.

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

Тема 1. Введение в информационную безопасность. Основные термины и определения.
□ Информация и её свойства □ Автоматизированная система и её ресурсы □ Доступ и его виды
Обзор проблемных областей информационной безопасности.

Тема 2. Подсистемы обеспечения информационной безопасности □ Криптографическая подсистема □ Подсистема управления доступом □ Подсистема обеспечения целостности □ Подсистема регистрации и учёта событий

Тема 3. Уязвимости, угрозы, атаки информационных систем и методы борьбы с ними. □ Угрозы безопасности информации в АС □ Классификация угроз и уязвимостей □ Анализ угроз АС □ Типовые угрозы безопасности □ Фазы атаки Сетевые атаки и способы защиты от них

Тема 4. Организационно-правовая поддержка деятельности администратора безопасности. □ Обзор законов и подзаконных актов РФ, связанных с обеспечением информационной безопасности □ Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации □ Пакет руководящих документов Гостехкомиссии России □ Специальные требования и рекомендации по технической защите конфиденциальной информации Особенности защиты персональных данных

Тема 5. Международные стандарты информационной безопасности: ИСО/МЭК 15408-2002, ISO17799 □ ISO 15408. Общие критерии □ Профили защиты □ Функциональные требования □ Требования доверия □ Особенности ISO 15408 по сравнению с другими стандартами в области безопасности Стандарт ISO 17799 и его структура. Анализ рисков

Тема 6. Политика информационной безопасности организации. □ Определения политики информационной безопасности □ Концепция информационной безопасности организации □ Локальные политики информационной безопасности и должностные инструкции □ Аварийный план

Тема 7. Обзор существующих средств защиты информации. Аттестация объектов информатизации. Проблема эксплуатации защищённых АС, администрирование безопасности информации АС. Виды деятельности, функции и задачи администрирования. Виды деятельности администратора КСЗ. Функции и задачи администрирования.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Разработанный блок вопросов для компьютерной системы тестирования ТСExam.

Вопросы к экзамену:

1. дайте определения

политика безопасности, профиль защиты, червь.

определение понятий идентификация, аутентификация, авторизация. Опишите механизм. Какие виды аутентификации вы знаете.

задание по безопасности, вирус, объект доступа.

блочный шифр, субъект доступа, автоматизированная система

группа, доступ, межсетевой экран

уязвимость, угроза, атака

безопасность информации, персонал, КСА

политика безопасности, аудит(все возможные трактовки), пользователи

определения всех видов обеспечения АС

2

Проведите сравнение ролевой и дискреционной моделей безопасностей, а так же приведите примеры, в каких сферах эти модели могут быть применены.

Обзор механизмов криптографической защиты информации

Обзор Руководящих документов Гостехкомиссии

Обзор стандартов информационной безопасности ИСО15408

Схемы ротации носителей информации.

Проведите сравнение ролевой и мандатной моделей безопасностей, а так же приведите примеры, в каких сферах эти модели могут быть применены.

Проведите сравнение дискреционной и мандатной моделей безопасностей, а так же приведите примеры. В каких сферах эти модели могут быть применены.

Обзор архитектур систем резервного копирования данных. Какие механизмы вы планируете там использовать и почему.

Обзор документа "СТР-К". Какие документы вы бы включили в политику безопасности.

7.1. Основная литература:

основная литература:

1. Зегжда П.Д. Теория и практика обеспечения информационной безопасности. - М.: Издательство Агентства "Яхтсмен", 1996.

2. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР). Решение Гостехкомиссии России от 23.05.97 г. ♦ 55-с.

3. ГОСТ Р.50922-96. Защита информации. Основные термины и определения.

4. РД. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение Председателя Гостехкомиссии России от 30.03.92 г.

5. РД. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Решение Председателя Гостехкомиссии России от 30.03.92 г.

6. РД. СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии России от 30.03.92 г.

7. РД. АС. Защита от НСД к информации. Классификация АС и требования по защите информации. Решение Председателя Гостехкомиссии России от 30.03.92 г.

8. РД. Защита от несанкционированного доступа (НСД) к информации. Термины и определения . Решения Председателя Гостехкомиссии России от 30.03.92 г.

9. РД. СВТ. Межсетевые экраны. Защита от НСД к информации . Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии России от 25.07.97 г.

10. ИСО/МЭК 15408-2002.

11. Чирилло Дж. Обнаружение хакерских атак (+ CD). Пер. с англ. - СПб.: Питер, 2003.
12. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. - СПб: Издательство "БХВ-Петербург", 2003.

7.2. Дополнительная литература:

1. А. И. Солонина, Д.А. Улахович, Л.А. Яковлев Цифровые процессоры обработки сигналов фирмы Motorola. СПб.: БХВ, 2000.
2. Модель ИТР-2010. Решение Гостехкомиссии России от 16.07.96 г. ♦49-с.
3. Методики оценки возможностей ИТР (МВТР-87 с изменениями). Решение Гостехкомиссии СССР от 16.09.87 г. ♦70-3.
4. Нормативно-методические документы по противодействию иностранной радиоразведке. Решение Гостехкомиссии России от 16.11.93 г. ♦7-с.
5. Скотт Бармен. Разработка правил информационной безопасности. - М.: Вильямс, 2002.
6. Расторгуев С. П. Основы информационной безопасности. Серия: Высшее профессиональное образование. Издательство: Академия, 2007.
7. Владимир Скиба, Владимир Курбатов Руководство по защите от внутренних угроз информационной безопасности. - СПб.: Питер, 2008.
8. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. Серия: Высшее профессиональное образование. Издательство: Академия, 2007.

7.3. Интернет-ресурсы:

8. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Освоение дисциплины "Физические основы защиты информации и информационная безопасность систем" предполагает использование следующего материально-технического обеспечения:

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по специальности: 010801.65 "Радиофизика и электроника" и специализации Защита информации .

Автор(ы):

Иванов К.В. _____

"__" _____ 201__ г.

Рецензент(ы):

"__" _____ 201__ г.