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

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Физические основы защиты информации и информационная безопасность&#65533; Б1.В.ДВ.7

Направление подготовки: 09.03.04 - Программная инженерия
Профиль подготовки: Технология проектирования аппаратно-программных информационных систем
Квалификация выпускника: бакалавр
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 6178519

Содержание

Программу дисциплины разработал(а)(и) Иванов К.В.

1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) Б1.В.ДВ.7 '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 "Б1.В.ДВ.7 Дисциплины (модули)" основной образовательной программы 09.03.04 Программная инженерия и относится к дисциплинам по выбору. Осваивается на 3, 4 курсах, 6, 7 семестры.

программы 09.03.04 'Программная инженерия 'Программно-аппаратные средства информационной безопасности' относится к дисциплинам Б1.В.ДВ.7

Осваивается на 4 курсе в 6-7 семестре.

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 осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий
ПК-16 (профессиональные компетенции)	способностью формализовать предметную область программного проекта и разработать спецификации для компонентов программного продукта
ПК-5 (профессиональные компетенции)	владением стандартами и моделями жизненного цикла
ПК-6 (профессиональные компетенции)	владением классическими концепциями и моделями менеджмента в управлении проектами
ПК-8 (профессиональные компетенции)	владением основами групповой динамики, психологии и профессионального поведения, специфичных для программной инженерии
ПК-21 (профессиональные компетенции)	владением навыками чтения, понимания и выделения главной идеи прочитанного исходного кода, документации
ПК-22 (профессиональные компетенции)	способностью создавать программные интерфейсы

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

4. должен демонстрировать способность и готовность:

применять полученные знания на практике

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 8 зачетных(ые) единиц(ы) 288 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 6 семестре; 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. 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	6	1-2	4	0	4	Отчет
2.	Тема 2. Подсистемы обеспечения информационной безопасности Криптографическая подсистема Подсистема управления доступом Подсистема обеспечения целостности Подсистема регистрации и учёта событий	6	3-5	4	0	4	Отчет

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные работы	
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	6	6-8	4	0	4	Отчет
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	6	9-11	6	0	6	Отчет
5.	Тема 5. Международные стандарты информационной безопасности: ИСО/МЭК 15408-2002, ISO17799 SO 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	6	12-14	6	0	6	Отчет
6.	Тема 6. Политика информационной безопасности организации. Определения политики информационной безопасности Концепция информационной безопасности организации Локальные политики информационной безопасности и должностные инструкции Аварийный план	6	15-16	6	0	6	Отчет

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные 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.	6	17-18	6	0	6	Отчет
8.	Тема 8. Программно-определяемые радиосистемы (SDR - software defined radio). Перепрограммируемые мульти-протокольные радиосистемы с использованием цифровой промежуточной частоты	7	1-3	2	0	0	Устный опрос
9.	Тема 9. Цифровые приемники с программной и аппаратной обработкой: SDR-приемники и DSP-приемники. Примеры конкретных приемников и их структура.	7	4-7	2	0	0	Устный опрос
10.	Тема 10. Программное обеспечение для конфигурации SDR-приемников и их использования для приема радиосигналов.	7	9-11	8	0	6	Компьютерная программа
11.	Тема 11. Структура типичного цифрового приемника на базе готовых DSP-микросхем. Аналоговый предварительный каскад (преселектор). Программное обеспечение для конфигурации и использования DSP-приемников	7	12-13	8	0	0	Устный опрос
12.	Тема 12. Реализация узлов цифрового приемника на ПЛИС: CIC и FIR фильтры, блоки подключения к АЦП (DFE - Digital Front End	7	14-15	8	0	6	Компьютерная программа
13.	Тема 13. Практическая регистрация сигналов различных радио-протоколов с помощью цифрового приемника.	7	16-17	8	0	6	Отчет

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные работы	
.	Тема . Итоговая форма контроля	6		0	0	0	Экзамен
.	Тема . Итоговая форма контроля	7		0	0	0	Экзамен
	Итого			72	0	54	

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

лекционное занятие (4 часа(ов)):

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

лабораторная работа (4 часа(ов)):

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

лекционное занятие (4 часа(ов)):

Подсистемы обеспечения информационной безопасности Криптографическая подсистема Подсистема управления доступом Подсистема обеспечения целостности Подсистема регистрации и учёта событий

лабораторная работа (4 часа(ов)):

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

лекционное занятие (4 часа(ов)):

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

лабораторная работа (4 часа(ов)):

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

лекционное занятие (6 часа(ов)):

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

лабораторная работа (6 часа(ов)):

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 SO 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

лекционное занятие (6 часа(ов)):

Международные стандарты информационной безопасности: ИСО/МЭК 15408-2002, ISO17799 SO 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

лабораторная работа (6 часа(ов)):

Международные стандарты информационной безопасности: ИСО/МЭК 15408-2002, ISO17799 SO 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

лекционное занятие (6 часа(ов)):

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

лабораторная работа (6 часа(ов)):

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.

лекционное занятие (6 часа(ов)):

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.

лабораторная работа (6 часа(ов)):

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 8. Программно-определяемые радиосистемы (SDR - software defined radio). Перепрограммируемые мульти-протокольные радиосистемы с использованием цифровой промежуточной частоты

лекционное занятие (2 часа(ов)):

Программно-определяемые радиосистемы (SDR - software defined radio). Перепрограммируемые мульти-стандартные радиосистемы с использованием цифровой промежуточной частоты. Концепция SDR - передача значительных объемов сигнальной обработки процессору общего назначения. Возможности современных процессоров общего назначения для обработки широкополосных сигналов УВЧ диапазона. Различия между SDR приемниками и передатчиками. Применение SDR-радиосистем как инструмента оптимального использования частотного диапазона (преодоления "ограниченного" спектра) с помощью: технологий широкополосного радиосигнала с размытым спектром и сверхширокополосных спектров; программного задания направления приема на антенном массиве (алгоритмы умной антенны и пространственной селекции помех); методов когнитивного радио; динамической регулировки мощности передатчика; создания интеллектуальной беспроводной сетки ретранслирующих узлов с минимальной длиной и мощностью. WEB SDR-приемники.

Тема 9. Цифровые приемники с программной и аппаратной обработкой: SDR-приемники и DSP-приемники. Примеры конкретных приемников и их структура.

лекционное занятие (2 часа(ов)):

Цифровые приемники с программной и аппаратной обработкой: SDR-приемники и DSP-приемники. Примеры конкретных приемников и их структура. Airspy, SDRplay, Ettus B200/B210, BladeRF, LimeSDR и трансиверы HackRF , SDR-1000 (FlexRadio Systems). Процессорные модули ADP/DSP и субмодули цифрового приема ADMDDC (АО "ИнСис")

Тема 10. Программное обеспечение для конфигурации SDR-приемников и их использования для приема радиосигналов.

лекционное занятие (8 часа(ов)):

Программное обеспечение для конфигурации и использования SDR. GNU Radio и его графы потока управления. Визуальная среда GNU Radio Companion (GRC). Основные блоки обработки сигналов - фильтры, элементы синхронизации, эквалайзеры, демодуляторы, декодеры, вокодеры. Область применения GRC: функционально сложные SDR, измерительные комплексы, DSP, цифровые фильтры, WEB-SDR, декодировать сложные сигналы (например изображения со спутников NOOA)

лабораторная работа (6 часа(ов)):

Программное обеспечение для конфигурации и использования SDR. GNU Radio и его графы потока управления. Визуальная среда GNU Radio Companion (GRC). Основные блоки обработки сигналов - фильтры, элементы синхронизации, эквалайзеры, демодуляторы, декодеры, вокодеры. Область применения GRC: функционально сложные SDR, измерительные комплексы, DSP, цифровые фильтры, WEB-SDR, декодировать сложные сигналы (например изображения со спутников NOOA)

Тема 11. Структура типичного цифрового приемника на базе готовых DSP-микросхем. Аналоговый предварительный каскад (преселектор). Программное обеспечение для конфигурации и использования DSP-приемников

лекционное занятие (8 часа(ов)):

Структура типичного цифрового приемника с перегружаемыми параметрами фильтров. Аналоговый предварительный каскад (AFE - analog front-end или RF front-end). Цифровой квадратурный гетеродин. Передискретизирующий интегрально-гребенчатый фильтр (CIC-фильтр cascaded integral-comb filters). Фильтр с конечной импульсной характеристикой, параметры которой хранятся на внутрикристальной памяти (RCF - RAM Coefficient FIR фильтр). Дециматор. Примеры интегрального исполнения AD6620/AD6634/AD6635/AD6652, HSP50016, GC4016, 1288XK1T

Тема 12. Реализация узлов цифрового приемника на ПЛИС: CIC и FIR фильтры, блоки подключения к АЦП (DFE - Digital Front End

лекционное занятие (8 часа(ов)):

Реализация узлов цифрового приемника на ПЛИС: CIC и FIR фильтры, блоки подключения к АЦП (DFE - Digital Front End). Цифровой квадратурный гетеродин. Передискретизирующий интегрально-гребенчатый фильтр (CIC-фильтр cascaded integral-comb filters). Фильтр с конечной импульсной характеристикой, параметры которой хранятся на внутрикристальной памяти (RCF - RAM Coefficient FIR фильтр). Дециматор.

лабораторная работа (6 часа(ов)):

Реализация узлов цифрового приемника на ПЛИС: CIC и FIR фильтры, блоки подключения к АЦП (DFE - Digital Front End). Цифровой квадратурный гетеродин. Передискретизирующий интегрально-гребенчатый фильтр (CIC-фильтр cascaded integral-comb filters). Фильтр с конечной импульсной характеристикой, параметры которой хранятся на внутрикристальной памяти (RCF - RAM Coefficient FIR фильтр). Дециматор. Разработка программы в среде Quartus узлов по декодированию сигналов с амплитудной и частотной модуляцией. Конкретные варианты заданий по виду модуляции (AM, SSB, FM, NFM, WFM) указывает преподаватель. Дополнительно указывается необходимость включения полосового фильтра, преобразования Гильберта, смены частоты дискретизации (передискретизации) и др.

Тема 13. Практическая регистрация сигналов различных радио-протоколов с помощью цифрового приемника.

лекционное занятие (8 часа(ов)):

Регистрация сигналов различных радио-протоколов с помощью цифрового приемника. Прием на различные цифровые приемники (процессорные модули АО "ИнСис", а также на простейшие RTL-SDR приемники) сигналы различных протоколов. В качестве источника сигналов используются как специализированные генераторы, а также радиосигналы, принимаемые на антенну.

лабораторная работа (6 часа(ов)):

Регистрация сигналов различных радио-протоколов с помощью цифрового приемника. Прием на различные цифровые приемники (процессорные модули АО "ИнСис", а также на простейшие RTL-SDR приемники) сигналы различных протоколов. В качестве источника сигналов используются как специализированные генераторы, а также радиосигналы, принимаемые на антенну.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной 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	6	1-2	подготовка к отчету	2	Отчет
2.	Тема 2. Подсистемы обеспечения информационной безопасности Криптографическая подсистема Подсистема управления доступом Подсистема обеспечения целостности Подсистема регистрации и учёта событий	6	3-5	подготовка к отчету	2	Отчет

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
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	6	6-8	подготовка к отчету	2	Отчет

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной 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	6	9-11	подготовка к отчету	2	Отчет

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
5.	Тема 5. Международные стандарты информационной безопасности: ИСО/МЭК 15408-2002, ISO17799 SO 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	6	12-14	подготовка к отчету	2	Отчет
6.	Тема 6. Политика информационной безопасности организации. Определения политики информационной безопасности Концепция информационной безопасности организации Локальные политики информационной безопасности и должностные инструкции Аварийный план	6	15-16	подготовка к отчету	4	Отчет

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной 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.	6	17-18	подготовка к отчету	4	Отчет
8.	Тема 8. Программно-определяемые радиосистемы (SDR - software defined radio). Перепрограммируемые мульти-протокольные радиосистемы с использованием цифровой промежуточной частоты	7	1-3	подготовка к устному опросу	2	Устный опрос
9.	Тема 9. Цифровые приемники с программной и аппаратной обработкой: SDR-приемники и DSP-приемники. Примеры конкретных приемников и их структура.	7	4-7	подготовка к устному опросу	4	Устный опрос

N	Раздел дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
10.	Тема 10. Программное обеспечение для конфигурации SDR-приемников и их использования для приема радиосигналов.	7	9-11		10	Компьютерная программа
11.	Тема 11. Структура типичного цифрового приемника на базе готовых DSP-микросхем. Аналоговый предварительный каскад (преселектор). Программное обеспечение для конфигурации и использования DSP-приемников	7	12-13	подготовка к устному опросу	12	Устный опрос
12.	Тема 12. Реализация узлов цифрового приемника на ПЛИС: CIC и FIR фильтры, блоки подключения к АЦП (DFE - Digital Front End	7	14-15		12	Компьютерная программа
13.	Тема 13. Практическая регистрация сигналов различных радио-протоколов с помощью цифрового приемника.	7	16-17	подготовка к отчету	14	Отчет
	Итого				72	

5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций читается на основе мультимедийных технологий, практические занятия проводятся в 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

Отчет , примерные вопросы:

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

Отчет , примерные вопросы:

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

Отчет , примерные вопросы:

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

Отчет , примерные вопросы:

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 SO 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

Отчет , примерные вопросы:

Международные стандарты информационной безопасности: ИСО/МЭК 15408-2002, ISO17799 SO 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

Отчет , примерные вопросы:

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.

Отчет , примерные вопросы:

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 8. Программно-определяемые радиосистемы (SDR - software defined radio). Перепрограммируемые мульти-протокольные радиосистемы с использованием цифровой промежуточной частоты

Устный опрос , примерные вопросы:

Программно-определяемые радиосистемы (SDR - software defined radio). Перепрограммируемые мульти-стандартные радиосистемы с использованием цифровой промежуточной частоты. Концепция SDR - передача значительных объемов сигнальной обработки процессору общего назначения. Возможности современных процессоров общего назначения для обработки широкополосных сигналов УВЧ диапазона. Различия между SDR приемниками и передатчиками. Применение SDR-радиосистем как инструмента оптимального использования частотного диапазона (преодоления "ограниченного" спектра) с помощью: технологий широкополосного радиосигнала с размытым спектром и сверхширокополосных спектров; программного задания направления приема на антенном массиве (алгоритмы умной антенны и пространственной селекции помех); методов когнитивного радио; динамической регулировки мощности передатчика; создания интеллектуальной беспроводной сетки ретранслирующих узлов с минимальной длиной и мощностью. WEB SDR-приемники.

Тема 9. Цифровые приемники с программной и аппаратной обработкой: SDR-приемники и DSP-приемники. Примеры конкретных приемников и их структура.

Устный опрос , примерные вопросы:

Цифровые приемники с программной и аппаратной обработкой: SDR-приемники и DSP-приемники. Примеры конкретных приемников и их структура. Airspy, SDRplay, Ettus B200/B210, BladeRF, LimeSDR и трансиверы HackRF , SDR-1000 (FlexRadio Systems). Процессорные модули ADP/DSP и субмодули цифрового приема ADMDDC (АО "ИнСис")

Тема 10. Программное обеспечение для конфигурации SDR-приемников и их использования для приема радиосигналов.

Компьютерная программа , примерные вопросы:

Программное обеспечение для конфигурации и использования SDR. GNU Radio и его графы потока управления. Визуальная среда GNU Radio Companion (GRC). Основные блоки обработки сигналов - фильтры, элементы синхронизации, эквалайзеры, демодуляторы, декодеры, вокодеры. Область применения GRC: функционально сложные SDR, измерительные комплексы, DSP, цифровые фильтры, WEB-SDR, декодировать сложные сигналы (например изображения со спутников NOOA)

Тема 11. Структура типичного цифрового приемника на базе готовых DSP-микросхем. Аналоговый предварительный каскад (преселектор). Программное обеспечение для конфигурации и использования DSP-приемников

Устный опрос , примерные вопросы:

Структура типичного цифрового приемника с перегружаемыми параметрами фильтров. Аналоговый предварительный каскад (AFE - analog front-end или RF front-end). Цифровой квадратурный гетеродин. Передискретизирующий интегрально-гребенчатый фильтр (CIC-фильтр cascaded integral-comb filters). Фильтр с конечной импульсной характеристикой, параметры которой хранятся на внутрикристальной памяти (RCF - RAM Coefficient FIR фильтр). Дециматор. Примеры интегрального исполнения AD6620/AD6634/AD6635/AD6652, HSP50016, GC4016, 1288XK1T

Тема 12. Реализация узлов цифрового приемника на ПЛИС: CIC и FIR фильтры, блоки подключения к АЦП (DFE - Digital Front End

Компьютерная программа , примерные вопросы:

Реализация узлов цифрового приемника на ПЛИС: CIC и FIR фильтры, блоки подключения к АЦП (DFE - Digital Front End). Цифровой квадратурный гетеродин. Передискретизирующий интегрально-гребенчатый фильтр (CIC-фильтр cascaded integral-comb filters). Фильтр с конечной импульсной характеристикой, параметры которой хранятся на внутрикристальной памяти (RCF - RAM Coefficient FIR фильтр). Дециматор

Тема 13. Практическая регистрация сигналов различных радио-протоколов с помощью цифрового приемника.

Отчет , примерные вопросы:

Регистрация сигналов различных радио-протоколов с помощью цифрового приемника. Прием на различные цифровые приемники (процессорные модули АО "ИнСис", а также на простейшие RTL-SDR приемники) сигналы различных протоколов. В качестве источника сигналов используются как специализированные генераторы, а также радиосигналы, принимаемые на антенну.

Итоговая форма контроля

экзамен (в 6 семестре)

Итоговая форма контроля

экзамен (в 7 семестре)

Примерные вопросы к итоговой форме контроля

Разработанный блок вопросов для компьютерной системы тестирования TCExam.

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:

1. Аверченков, В. И. Защита персональных данных в организации [электронный ресурс] : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. - 2-е изд., стереотип. - М.: Флинта, 2011. - 124 с. - Режим доступа: http://znanium.com/bookread2.php?book=453736

2. Программно-аппаратная защита информации: учеб. пособие / П.Б. Хорев. - 2-е изд., испр. и доп. ? М. : ФОРУМ : ИНФРА-М, 2019. - 352 с. - (Высшее образование). - Режим доступа: http://znanium.com/catalog/product/1025261

3. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М. : ФОРУМ : ИНФРА-М, 2019.- 432 с. - Режим доступа: http://znanium.com/catalog/product/987326

4. Основные положения информационной безопасности: учеб. пособие / В.Я. Ищейнов, М.В. Мецатунян. - М. : ФОРУМ : ИНФРА-М, 2018. - 208 с.- Режим доступа: http://znanium.com/catalog/product/927190

5. Галкин В.А., Основы программно-конфигурируемого радио [Электронный ресурс] / Галкин В.А. - М.: Горячая линия - Телеком, 2013. - 372 с. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203050.html

6. Рембовский А.М., Радиомониторинг: задачи, методы, средства [Электронный ресурс] / Под ред. А.М. Рембовского. - 3-е изд., перераб. и доп. - М.: Горячая линия - Телеком, 2012. - 640 с. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202367.html

7.2. Дополнительная литература:

1. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. - М.: ИД 'ФОРУМ' : ИНФРА-М, 2019. - 592 с. - (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/996789

2. 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.- Режим доступа: http://znanium.com/bookread.php?book=405000

3. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. - М. : ИД 'ФОРУМ' : ИНФРА-М, 2019. - 416 с. - Режим доступа: http://znanium.com/catalog/product/1009605

4. Дятлов А.П., Корреляционная обработка широкополосных сигналов в автоматизированных комплексах радиомониторинга [Электронный ресурс] / Дятлов А.П., Кульбикаян Б.Х - М. : Горячая линия - Телеком, 2013. - 332 с. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203326.html

5. Киселев Д.Н., Радиомониторинг и распознавание радиоизлучений [Электронный ресурс]: Учебное пособие для вузов. / О.Ю. Перфилов, Д.Н. Киселев - М. : Горячая линия - Телеком, 2015. - 90 с. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204903.html

6. Трушин В.А., Радиомониторинг. Исследование возможностей и особенностей применения программно-аппаратного комплекса С2М [Электронный ресурс]: учебно-методическое пособие / Трушин В.А. - Новосибирск: Изд-во НГТУ. - 28 с. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778232778.html

7.3. Интернет-ресурсы:

Lan Agent - мониторинг компьютеров ЛС - http://www.lanagent.ru/

Интеллект-сервис - http://www.it-ic.ru/

Стандарты информационной безопасности - http://www.arinteg.ru/articles/standarty-informatsionnoy-bezopasnosti-27697.html

Федеральная служба по техническому и экспортному контролю - http://fstec.ru/

Школа IT-менеджмента - http://www.itmane.ru/mba-cso

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Физические основы защиты информации и информационная безопасность&#65533;" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента" , доступ к которой предоставлен студентам. Электронная библиотечная система "Консультант студента" предоставляет полнотекстовый доступ к современной учебной литературе по основным дисциплинам, изучаемым в медицинских вузах (представлены издания как чисто медицинского профиля, так и по естественным, точным и общественным наукам). ЭБС предоставляет вузу наиболее полные комплекты необходимой литературы в соответствии с требованиями государственных образовательных стандартов с соблюдением авторских и смежных прав.

Освоение дисциплины "Физические основы защиты информации и информационная безопасность" 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 09.03.04 "Программная инженерия" и профилю подготовки Технология проектирования аппаратно-программных информационных систем .

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

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