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.

# Программа дисциплины

Физические основы защиты информации и информационная безопасность Б1.В.ДВ.12

Направление подготовки: 03.03.03 - Радиофизика
Профиль подготовки: Специальные радиотехнические системы
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

Казань
2018

## Содержание

Программу дисциплины разработал(а)(и) Иванов К.В. , KVIvanov@kpfu.ru

## 1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) Б1.В.ДВ.12 '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.12 Дисциплины (модули)" основной образовательной программы 03.03.03 Радиофизика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 7 семестр.

Данная учебная дисциплина включена в раздел ' Б1.В.ДВ.12 Профессиональный' основной образовательной программы 03.03.03 Радиофизика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 7 семестр.

Дисциплина Б1.В.ДВ.12 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:

| Шифр компетенции | Расшифровка приобретаемой компетенции |
|---|---|
| ОК-12 (общекультурные компетенции) | способностью к правильному использованию общенаучной и специальной терминологии |
| ОК-14 (общекультурные компетенции) | способностью к овладению базовыми знаниями в области информатики и современных информационных технологий, программными средствами и навыками работы в компьютерных сетях, использованию баз данных и ресурсов Интернет |
| ПК-2 (профессиональные компетенции) | способностью применять на практике базовые профессиональные навыки |
| ПК-3 (профессиональные компетенции) | способностью понимать принципы работы и методы эксплуатации современной радиоэлектронной и оптической аппаратуры и оборудования |
| ПК-5 (профессиональные компетенции) | способностью к владению компьютером на уровне опытного пользователя, применению информационных технологий для решения задач в области радиотехники, радиоэлектроники и радиофизики (в соответствии с профилизацией) |

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 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 7 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

### 4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

**Тематический план дисциплины/модуля**

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практические занятия | Лабораторные работы | |
| 1. | Тема 1. 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 | 7 | 1-2 | 4 | 4 | 0 | Отчет |

| 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. Подсистемы обеспечения информационной безопасности Криптографическая подсистема Подсистема управления доступом Подсистема обеспечения целостности Подсистема регистрации и учёта событий | 7 | 3-5 | 4 | 4 | 0 | Отчет |
| 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 | 7 | 6-8 | 4 | 4 | 0 | Отчет |

| 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 | 7 | 9-11 | 4 | 6 | 0 | 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 | 7 | 12-14 | 4 | 6 | 0 | Отчет |

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практические занятия | Лабораторные работы | |
| 6. | Тема 6. Политика информационной безопасности организации. Определения политики информационной безопасности Концепция информационной безопасности организации Локальные политики информационной безопасности и должностные инструкции Аварийный план | 7 | 15-16 | 2 | 6 | 0 | Отчет |
| 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. | 7 | 17-18 | 2 | 6 | 0 | Отчет |
| . | Тема . Итоговая форма контроля | 7 | | 0 | 0 | 0 | Экзамен |
| | Итого | | | 24 | 36 | 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**

***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

***практическое 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

**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

***практическое занятие (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

***практическое 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

**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 (4 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

***практическое 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

**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 (4 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

***практическое 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

**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 (2 часа(ов)):***

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

***практическое 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

**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 (2 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.

***практическое 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.

### 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. 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 | 7 | 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 | 7 | 3-5 | подготовка к отчету | 2 | Отчет |
| 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 | 7 | 6-8 | подготовка к отчету | 2 | Отчет |

| N | Раздел Дисциплины | Семестр | Неделя семестра | Виды самостоятельной работы студентов | Трудоемкость (в часах) | Формы контроля самостоятельной 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 | 7 | 9-11 | подготовка к отчету | 2 | 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 | 7 | 12-14 | подготовка к отчету | 2 | Отчет |

| N | Раздел Дисциплины | Семестр | Неделя семестра | Виды самостоятельной работы студентов | Трудоемкость (в часах) | Формы контроля самостоятельной работы |
|---|---|---|---|---|---|---|
| 6. | Тема 6. Политика информационной безопасности организации. Определения политики информационной безопасности Концепция информационной безопасности организации Локальные политики информационной безопасности и должностные инструкции Аварийный план | 7 | 15-16 | подготовка к отчету | 2 | Отчет |
| | Итого | | | | 12 | |

## 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.**

**Тема . Итоговая форма контроля**

Примерные вопросы к экзамену:

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. 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:

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" 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 Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех 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 03.03.03 "Радиофизика" и профилю подготовки Специальные радиотехнические системы .

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

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