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



*подписано электронно-цифровой подписью*

# Программа дисциплины

Программно-аппаратные средства информационной безопасности Б3.ДВ.8

Направление подготовки: 011800.62 - 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 626314

Казань
2014

## Содержание

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

в данном курсе рассматриваются основные принципы, лежащие в основе построения аппаратных средств современной электронно-вычислительной техники, особое внимание при этом уделяется реализации этих принципов на примере персонального компьютера.

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

Данная учебная дисциплина включена в раздел " Б3.ДВ.8 Профессиональный" основной образовательной программы 011800.62 Радиофизика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 7 семестр.

Дисциплина Б3.ДВ8. " Программно-аппаратные средства информационной безопасности " 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 |
| ОК-15 (общекультурные компетенции) | способностью получить организационно-управленческие навыки |
| ОК-16 (общекультурные компетенции) | способностью овладения основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий |
| 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) |
| ПК-6 (профессиональные компетенции) | способностью к профессиональному развитию и саморазвитию в области радиофизики и электроники |

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 на практике

## 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 72 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. 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.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 7 | | 2 | 0 | 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. Операционная система (ОС) Linux и её подсистема безопасности. Методика и практика использования систем на базе Linux. Возможности комплекса средств защиты (КСЗ) ОС. Подсистема разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема. | 7 | | 4 | 3 | 0 | отчет |
| 3. | Тема 3. 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 | 7 | | 4 | 3 | 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. Построение подсистемы антивирусной защиты. Классификация вредоносного программного обеспечения (ПО). Обзор существующих методов и средств антивирусной защиты. Стратегии антивирусной защиты. | 7 | | 2 | 3 | 0 | отчет |
| 5. | Тема 5. Использование добавочных средств защиты. Средства резервного копирования информации. Виртуальные частные сети. | 7 | | 6 | 3 | 0 | отчет |
| 6. | Тема 6. Построение систем межсетевого экранирования. Межсетевые экраны на безе ОС Windows и Linux. Создание системы обнаружения вторжений. | 7 | | 4 | 3 | 0 | отчет |
| 7. | Тема 7. Средства защиты информации активного сетевого оборудования. Списки контроля доступа. Виртуальные локальные сети. | 7 | | 2 | 3 | 0 | отчет |
| 8. | Тема 8. Использование средств анализа защищённости. | 7 | | 2 | 3 | 0 | отчет |
| 9. | Тема . Итоговая форма контроля | 7 | | 0 | 0 | 0 | экзамен |
| | Итого | | | 24 | 18 | 0 | |

**4.2 Содержание дисциплины**

**Тема 1. 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.**

***лекционное занятие (2 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.

**Тема 2. Операционная система (ОС) Linux и её подсистема безопасности. Методика и практика использования систем на базе Linux. Возможности комплекса средств защиты (КСЗ) ОС. Подсистема разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема.**

***лекционное занятие (4 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 разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема.

***практическое занятие (3 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 разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема.

**Тема 3. 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**

***лекционное занятие (4 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 (3 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

**Тема 4. Построение подсистемы антивирусной защиты. Классификация вредоносного программного обеспечения (ПО). Обзор существующих методов и средств антивирусной защиты. Стратегии антивирусной защиты.**

***лекционное занятие (2 часа(ов)):***

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

***практическое занятие (3 часа(ов)):***

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

**Тема 5. Использование добавочных средств защиты. Средства резервного копирования информации. Виртуальные частные сети.**

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

Использование добавочных средств защиты. Средства резервного копирования информации. Виртуальные частные сети.

***практическое занятие (3 часа(ов)):***

Использование добавочных средств защиты. Средства резервного копирования информации. Виртуальные частные сети.

**Тема 6. Построение системы межсетевого экранирования. Межсетевые экраны на безе ОС Windows и Linux. Создание системы обнаружения вторжений.**

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

Построение системы межсетевого экранирования. Межсетевые экраны на безе ОС Windows и Linux. Создание системы обнаружения вторжений.

***практическое занятие (3 часа(ов)):***

Построение системы межсетевого экранирования. Межсетевые экраны на безе ОС Windows и Linux. Создание системы обнаружения вторжений.

**Тема 7. Средства защиты информации. активного сетевого оборудования. Списки контроля доступа. Виртуальные локальные сети. Использование инструментальных средств анализа защищённости.**

***лекционное занятие (2 часа(ов)):***

Средства защиты информации. активного сетевого оборудования. Списки контроля доступа. Виртуальные локальные сети. Использование инструментальных средств анализа защищённости.

***практическое занятие (3 часа(ов)):***

Средства защиты информации. активного сетевого оборудования. Списки контроля доступа. Виртуальные локальные сети. 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. 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. | 7 | | подготовка к отчету | 6 | отчет |
| 2. | Тема 2. Операционная система (ОС) Linux и её подсистема безопасности. Методика и практика использования систем на базе Linux. Возможности комплекса средств защиты (КСЗ) ОС. Подсистема разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема. | 7 | | подготовка к отчету | 4 | отчет |

| N | Раздел Дисциплины | Семестр | Неделя семестра | Виды самостоятельной работы студентов | Трудоемкость (в часах) | Формы контроля самостоятельной работы |
|---|---|---|---|---|---|---|
| 3. | Тема 3. 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 | 7 | | подготовка к отчету | 4 | отчет |
| 4. | Тема 4. Построение подсистемы антивирусной защиты. Классификация вредоносного программного обеспечения (ПО). Обзор существующих методов и средств антивирусной защиты. Стратегии антивирусной защиты. | 7 | | подготовка к отчету | 4 | отчет |
| 5. | Тема 5. Использование добавочных средств защиты. Средства резервного копирования информации. Виртуальные частные сети. | 7 | | подготовка к отчету | 4 | отчет |
| 6. | Тема 6. Построение системы межсетевого экранирования. Межсетевые экраны на безе ОС Windows и Linux. Создание системы обнаружения вторжений. | 7 | | подготовка к отчету | 4 | отчет |

| N | Раздел Дисциплины | Семестр | Неделя семестра | Виды самостоятельной работы студентов | Трудоемкость (в часах) | Формы контроля самостоятельной работы |
|---|---|---|---|---|---|---|
| 7. | Тема 7. Средства защиты информации. активного сетевого оборудования. Списки контроля доступа. Виртуальные локальные сети. Использование инструментальных средств анализа защищённости. | 7 | | подготовка к отчету | 4 | отчет |
| | Итого | | | | 30 | |

## 5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций читается на основе мультимедийных технологий.

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

**Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем. Жизненный цикл корпоративный системы. Обзор подходов к созданию защищённых автоматизированных систем (АС). Проблемы проектирования и реализации защищенных АС. Синтез АС и его этапы.**

отчет , примерные вопросы:

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.

**Тема 2. Операционная система (ОС) Linux и её подсистема безопасности. Методика и практика использования систем на базе Linux. Возможности комплекса средств защиты (КСЗ) ОС. Подсистема разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема.**

отчет , примерные вопросы:

Операционная система (ОС) Linux и её подсистема безопасности. Методика и практика использования систем на базе Linux. Возможности комплекса средств защиты (КСЗ) ОС. Подсистема разграничения доступа. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема.

**Тема 3. 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**

отчет , примерные вопросы:

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

**Тема 4. Построение подсистемы антивирусной защиты. Классификация вредоносного программного обеспечения (ПО). Обзор существующих методов и средств антивирусной защиты. Стратегии антивирусной защиты.**

отчет , примерные вопросы:

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

**Тема 5. Использование добавочных средств защиты. Средства резервного копирования информации. Виртуальные частные сети.**

отчет , примерные вопросы:

Использование добавочных средств защиты. Средства резервного копирования информации. Виртуальные частные сети.

**Тема 6. Построение системы межсетевого экранирования. Межсетевые экраны на безе ОС Windows и Linux. Создание системы обнаружения вторжений.**

отчет , примерные вопросы:

Построение системы межсетевого экранирования. Межсетевые экраны на безе ОС Windows и Linux. Создание системы обнаружения вторжений.

**Тема 7. Средства защиты информации. активного сетевого оборудования. Списки контроля доступа. Виртуальные локальные сети. Использование инструментальных средств анализа защищённости.**

отчет , примерные вопросы:

Средства защиты информации. активного сетевого оборудования. Списки контроля доступа. Виртуальные локальные сети. Использование инструментальных средств анализа защищённости.

**Тема . Итоговая форма контроля**

Примерные вопросы к экзамену:

Разработанный блок вопросов для компьютерной системы тестирования TCExam.

Вопросы к экзамену

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. Построение подсистемы антивирусной защиты
6.Межсетевые экраны. определение, назначение, классификации.
7. Архитектура систем активного аудита
8.Обзор инструментальных средств анализа защищённости АС
9. Средства защиты информации. активного сетевого оборудования

Форма контроля - экзамен.

### 7.1. Основная литература:

Бабаш А. В. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013.

http://znanium.com/bookread.php?book=405000

Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с.: http://znanium.com/bookread.php?book=169345

Аверченков В И Рытов М. Ю. Аверченков, В. И. Организационная защита информации [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - 3-е изд., стереотип. - М. : ФЛИНТА, 2011. - 184 с. : http://znanium.com/bookread.php?book=453862

### 7.2. Дополнительная литература:

Казарин О. В. Методология защиты программного обеспечения: Москва Изд-во МЦНМО 2009

Партыка Т. Л. Попов И. И. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2008. URL: http://znanium.com/catalog.php?bookinfo=167284

### 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 экспортномцу контролю - http://www.fstec.ru//

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

### 8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Программно-аппаратные средства информационной безопасности" предполагает использование следующего материально-технического обеспечения:

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 011800.62 "Радиофизика" и профилю подготовки Специальные радиотехнические системы .

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

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