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.

*подписано электронно-цифровой подписью*

# Программа дисциплины

Программно-аппаратные средства информационной безопасности Б3.ДВ.11

Направление подготовки: 011800.62 - Радиофизика
Профиль подготовки: Физика ионосферы и распространения радиоволн, радиоастрономия
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

**Автор(ы):**
Иванов К.В.

**Рецензент(ы):**
Корчагин П.А.

**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 694317

Казань
2017

## Содержание

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

## 1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) Б3.ДВ11. "Программно-аппаратные средства информационной безопасности " является получение теоретических знаний о функционировании современных средств защиты информации и практических навыков администрирования этих средств.

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

Данная учебная дисциплина включена в раздел " Б3.ДВ.11 Профессиональный" основной образовательной программы 011800.62 Радиофизика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 8 семестр.

Дисциплина Б3.ДВ11. " 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) | способность к правильному использованию общенаучной и специальной терминологии |
| ОК-14 (общекультурные компетенции) | способность 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) | способность получить организационно-управленческие навыки |
| ОК-16 (общекультурные компетенции) | способность овладения основными методами защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий |
| ПК-2 (профессиональные компетенции) | способность 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) | способность 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) | способность 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:

решать задачи, связанные с выбором, установкой и настройкой средств защиты информации

## 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 5 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 8 семестре.

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

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

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

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

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

**Тематический план дисциплины/модуля**

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практические занятия | Лабораторные работы | |
| 1. | Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем. | 8 | 1-3 | 6 | 0 | 0 | Устный опрос |
| 2. | Тема 2. Операционная система (ОС) Linux и её подсистема безопасности. | 8 | 4-5 | 4 | 0 | 10 | Устный опрос |

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|---|---|---|---|---|---|---|---|
| | | | | Лекции | Практические занятия | Лабораторные работы | |
| 3. | Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности. | 8 | 6-7 | 4 | 0 | 10 | Устный опрос |
| 4. | Тема 4. Построение подсистемы антивирусной защиты. | 8 | 8 | 2 | 0 | 4 | Устный опрос |
| 5. | Тема 5. Использование добавочных средств защиты. | 8 | 9-11 | 6 | 0 | 4 | Устный опрос |
| 6. | Тема 6. Построение системы межсетевого экранирования. | 8 | 12-14 | 6 | 0 | 4 | Устный опрос |
| 7. | Тема 7. Средства защиты информации. активного сетевого оборудования. | 8 | 15-18 | 8 | 0 | 4 | Устный опрос |
| . | Тема . Итоговая форма контроля | 8 | | 0 | 0 | 0 | Экзамен |
| | Итого | | | 36 | 0 | 36 | |

**4.2 Содержание дисциплины**

**Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем.**

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

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.**

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

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.

***лабораторная работа (10 часа(ов)):***

Установка и настройка ОС RedHat, изучение возможностей подсистемы разграничения доступа, настройка подсистемы регистрации и учета, подсистемы обеспечения целостности.

**Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.**

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

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

***лабораторная работа (10 часа(ов)):***

Установка и настройка ОС Windows 2008 Server, изучение возможностей подсистемы разграничения доступа, настройка подсистемы регистрации и учета, подсистемы обеспечения целостности. Работа с интерфейсом администратора безопасности.

**Тема 4. Построение подсистемы антивирусной защиты.**

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

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

***лабораторная работа (4 часа(ов)):***

Установка и настройка антивирусной защиты на основе Kaspersky Business Space Security.

**Тема 5. Использование добавочных средств защиты.**

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

Понятие встроенной и добавочной защиты. Средства резервного копирования информации. Виртуальные частные сети.

***лабораторная работа (4 часа(ов)):***

Настройка средств резервного копирования. Моделирование виртуальных частных сетей на предприятии.

**Тема 6. Построение системы межсетевого экранирования.**

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

Классификации и реализации межсетевых экранов. Межсетевые экраны на безе ОС Windows и Linux. Создание системы обнаружения вторжений.

***лабораторная работа (4 часа(ов)):***

Установка и настройка межсетевого экрана iptables. Реализация системы обнаружения вторжений на примере Suricata IDS.

**Тема 7. Средства защиты информации. активного сетевого оборудования.**

***лекционное занятие (8 часа(ов)):***

Списки контроля доступа. Виртуальные локальные сети. Использование инструментальных средств анализа защищённости.

***лабораторная работа (4 часа(ов)):***

Использование сканера уязвимостей Nessus для анализа защищенности предприятия.

### 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. | 8 | 1-3 | подготовка к написанию отчёта | 8 | отчёт |
| | | | | подготовка к устному опросу | 2 | устный опрос |
| 2. | Тема 2. Операционная система (ОС) Linux и её подсистема безопасности. | 8 | 4-5 | подготовка к написанию отчёта | 10 | отчёт |
| | | | | подготовка к устному опросу | 4 | устный опрос |
| 3. | Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности. | 8 | 6-7 | подготовка к написанию отчёта | 10 | отчёт |
| | | | | подготовка к устному опросу | 4 | устный опрос |

| N | Раздел Дисциплины | Семестр | Неделя семестра | Виды самостоятельной работы студентов | Трудоемкость (в часах) | Формы контроля самостоятельной работы |
|---|---|---|---|---|---|---|
| 4. | Тема 4. Построение подсистемы антивирусной защиты. | 8 | 8 | подготовка к написанию отчёта | 4 | отчёт |
| | | | | подготовка к устному опросу | 2 | устный опрос |
| 5. | Тема 5. Использование добавочных средств защиты. | 8 | 9-11 | подготовка к написанию отчёта | 6 | отчёт |
| | | | | подготовка к устному опросу | 2 | устный опрос |
| 6. | Тема 6. Построение системы межсетевого экранирования. | 8 | 12-14 | подготовка к написанию отчёта | 8 | отчёт |
| | | | | подготовка к устному опросу | 2 | устный опрос |
| 7. | Тема 7. Средства защиты информации. активного сетевого оборудования. | 8 | 15-18 | подготовка к написанию отчёта | 8 | отчёт |
| | | | | подготовка к устному опросу | 2 | устный опрос |
| | Итого | | | | 72 | |

## 5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций читается на основе мультимедийных технологий,.

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

**Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем.**

отчёт , примерные вопросы:

Отчет и технический проект с выбранным набором нормативных документов для реализации системы защиты информации предприятия.

устный опрос , 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.**

отчёт , примерные вопросы:

Отчет об установке и настройке ОС RedHat, настройки подсистемы разграничения доступа, подсистемы регистрации и учета, подсистемы обеспечения целостности.

устный опрос , 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.**

отчёт , примерные вопросы:

Отчет об установке и настройке ОС Windows 2008 Server, изучении возможностей подсистемы разграничения доступа, настройке подсистемы регистрации и учета, подсистемы обеспечения целостности. Описание элементов интерфейса администратора безопасности использованных в ходе работы.

устный опрос , 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.**

отчёт, примерные вопросы:

Отчет об установке и настройке антивирусной защиты на основе Kaspersky Business Space Security.

устный опрос , 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.**

отчёт , примерные вопросы:

Отчет о настройке средств резервного копирование. Моделирование виртуальных частных сетей на предприятии.

устный опрос , примерные вопросы:

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

**Тема 6. Построение системы межсетевого экранирования.**

отчёт , примерные вопросы:

Отчет об установке и настройке межсетевого экрана iptables и реализации системы обнаружения вторжений на примере Suricata IDS.

устный опрос , 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.**

отчёт , примерные вопросы:

Отчет сканера уязвимостей Nessus и подготовка рекомендаций для анализа защищенности предприятия на основе выявленных нарушений.

устный опрос , 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:

1. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: http://znanium.com/bookread.php?book=474838

2. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. http://znanium.com/bookread.php?book=432654

3. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. http://znanium.com/bookread.php?book=476047

4. Партыка Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. http://znanium.com/bookrea,d.php?book=420047

5.Молдовян Н. А. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - СПб.: БХВ-Петербург, 2010. - 293 с. - (Учебное пособие) http://znanium.com/bookread.php?book=351283

### 7.2. Дополнительная литература:

1.Чмора А. Л.. Современная прикладная криптография: Учеб. пособие : Гелиос АРВ, 2001.256с.:

2. Лопатин В. Н. Информационная безопасность России: СПб.: Фонд "Университет", 2000. 426с..

3. Бабаш, А. В. Криптография М.: СОЛОН-Р, 2002.?509с.

4. Левин М. Криптография: Руководство пользователя М.: Познавательная книга плюс, 2001.319с.

5. Столлингс В. Основы защиты сетей. Приложения и стандарты ?М.: Издат. Дом "Вильямс", 2002.429с

6. Столлингс, Вильям. Криптография и защита сетей. Принципы и практика ?М.: Издат. Дом "Вильямс", 2001.669с.:

### 7.3. Интернет-ресурсы:

Всё об инфрмационных систмах персональных данных - http://www.ispdn.ru/

Искусство управления информационной безопасностью - http://iso27000.ru/

Сайт федеральной службы по техническому и экспортному контролю - http://fstec.ru/

Центр безопасности Microsoft - http://www.microsoft.com/ru-ru/security/default.aspx

Эшелон. Комплексная безопасность - http://s3r.ru/

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

Освоение дисциплины "Программно-аппаратные средства информационной безопасности" 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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Компьютерный класс, позволяющий развёртывать на каждой ЭВМ не менее 2 виртуальных машин.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 011800.62 "Радиофизика" и профилю подготовки Физика ионосферы и распространения радиоволн, радиоастрономия .

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

Рецензент(ы):
Корчагин П.А. _____
"__" _____ 201 __ г.