

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Высшая школа информационных технологий и информационных систем



подписано электронно-цифровой подписью

Программа дисциплины
Информационная безопасность БЗ.Б.3.5

Направление подготовки: 230700.62 - Прикладная информатика

Профиль подготовки: не предусмотрено

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 Высшей школы информационных технологий и информационных систем:

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

Регистрационный No 68957714

Казань
2014

Содержание

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

Программу дисциплины разработал(а)(и) ассистент, к.н. Иванов К.В. Кафедра радиоастрономии Отделение радиофизики и информационных систем , KVIvanov@kpfu.ru

1. Цели освоения дисциплины

Цель курса:

- Введение в проблему построения защищённых информационных систем, изучение угроз безопасности информации, возникающих в таких системах, а также их уязвимостей и атак на них;
- Рассмотреть общедоступные возможности по оценке уровня защищённости информационных систем и устранению недостатков;
- Дать обзор теоретических основ защиты информации и примеров реализации механизмов защиты для операционных систем, сетей передачи данных и приложений;

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

Данная учебная дисциплина включена в раздел " Б3.Б.3 Профессиональный" основной образовательной программы 230700.62 Прикладная информатика и относится к базовой (общепрофессиональной) части. Осваивается на 4 курсе, 7 семестр.

Данная дисциплина "Информационная безопасность" входит в состав профессиональных дисциплин Б 3.Б.2.5, читается на 4 курсе в 7 семестре. Знания, полученные при изучении этой дисциплине, потребуются далее при изучении таких дисциплин как "Проектирование информационных систем", " Операционные системы" и др., а также при написании выпускных квалификационных работ.

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

В результате освоения дисциплины формируются следующие компетенции:

| Шифр компетенции | Расшифровка приобретаемой компетенции |
|---|---|
| ОК-11 (общекультурные компетенции) | способен уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия |
| ОК-13 (общекультурные компетенции) | способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны |
| ОК-14 (общекультурные компетенции) | способен применять основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий, технику безопасности на производстве |
| ПК-1 (профессиональные компетенции) | способен использовать нормативные правовые документы в профессиональной деятельности |
| ПК-18 (профессиональные компетенции) | способен анализировать и выбирать методы и средства обеспечения информационной безопасности |

| Шифр компетенции | Расшифровка приобретаемой компетенции |
|--|---|
| ПК-3 (профессиональные компетенции) | способен использовать основные законы естественнонаучных дисциплин в профессиональной деятельности и эксплуатировать современное электронное оборудование и информационно-коммуникационные технологии в соответствии с целями образовательной программы бакалавра |

В результате освоения дисциплины студент:

1. должен знать:

Должен знать:

- угрозы безопасности информации и уязвимости сетевого оборудования, системного и прикладного программного обеспечения;
- технологии защиты информации, применяемые при построении информационных систем, защите персональных компьютеров, серверов и мобильных устройств,
- основное содержание, средства и методы используемых на практике или используемых на практике или развиваемых направлений информационной защиты,
- основные механизмы защиты информации,
- принципы комплексирования средств и методов защиты информации.

2. должен уметь:

Должен уметь:

- Разбираться в терминологии по защите информации;
- Выявлять уязвимости прикладного и системного программного обеспечения;
- Проводить настройку механизмов защиты информации, реализованных в операционных системах;
- Проектировать программное обеспечение с учётом необходимости реализации механизмов защиты информации.

3. должен владеть:

Владеть:

- навыками практического выявления уязвимостей и минимизации последствий их использования;
- навыками настройки механизмов защиты информации, реализованных в операционных системах;

4. должен демонстрировать способность и готовность:

- Применять программно-технические способы и средства для обеспечения информационной безопасности объекта.
- Проектировать программное обеспечение с учётом необходимости реализации механизмов защиты информации.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины зачет 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. Основные вопросы защиты информации | 7 | 1-2 | 2 | 0 | 0 | устный опрос |
| 2. | Тема 2. Уязвимости, угрозы, атаки и их классификации | 7 | 2-3 | 2 | 0 | 0 | устный опрос |
| 3. | Тема 3. Теоретические основы защиты информации | 7 | 4-5 | 2 | 0 | 0 | контрольная работа |
| 4. | Тема 4. Возможности сканеров уязвимостей | 7 | 6-7 | 2 | 6 | 0 | отчет |
| 5. | Тема 5. Механизмы защиты информации, реализованные в ОС семейства Windows | 7 | 8-9 | 2 | 8 | 0 | тестирование отчет |
| 6. | Тема 6. Механизмы защиты информации, реализованные в ОС семейства Linux | 7 | 10-13 | 2 | 8 | 0 | отчет тестирование |
| 7. | Тема 7. Механизмы защиты информации, реализованные в прикладном программном обеспечении | 7 | 14-16 | 2 | 7 | 0 | отчет тестирование |

| N | Раздел Дисциплины/ Модуля | Семестр | Неделя семестра | Виды и часы аудиторной работы, их трудоемкость (в часах) | | | Текущие формы контроля |
|----|--|---------|--------------------|---|-------------------------|------------------------|--------------------------------|
| | | | | Лекции | Практические занятия | Лабораторные работы | |
| 8. | Тема 8. Механизмы защиты информации, реализованные в активном сетевом оборудовании | 7 | 17-18 | 4 | 7 | 0 | отчет контрольная работа |
| | Тема . Итоговая форма контроля | 7 | | 0 | 0 | 0 | зачет |
| | Итого | | | 18 | 36 | 0 | |

4.2 Содержание дисциплины

Тема 1. Основные вопросы защиты информации

лекционное занятие (2 часа(ов)):

1.1. Введение в информационную безопасность. 1.2. Уровни представления информации и особенности ее защиты. 1.3. Основные термины и определения. 1.4. Реализация информационной защиты.

Тема 2. Уязвимости, угрозы, атаки и их классификации

лекционное занятие (2 часа(ов)):

2.1. Уязвимости и их классификация. 2.2. Угрозы и их классификация 2.3. Атаки, их разновидности и методы защиты от них

Тема 3. Теоретические основы защиты информации

лекционное занятие (2 часа(ов)):

3.1 Механизмы подсистемы управления доступом 3.2. Механизмы криптографической подсистемы 3.3. Механизмы подсистемы регистрации и учёта событий 3.4. Механизмы подсистемы обеспечения целостности

Тема 4. Возможности сканеров уязвимостей

лекционное занятие (2 часа(ов)):

4.1. Определение и классификация сканеров уязвимостей. 4.2 Структура сканера уязвимостей. 4.3 Сценарии применения сканеров уязвимостей

практическое занятие (6 часа(ов)):

Использование инструментальных средств анализа защищённости. Установка и использование сканера Nessus.

Тема 5. Механизмы защиты информации, реализованные в ОС семейства Windows

лекционное занятие (2 часа(ов)):

5.1 Операционные системы семейства Windows и их подсистемы безопасности. 5.2 Компоненты системы безопасности. 5.3 Система безопасности Windows XP Professional и Windows Server 2003 5.4. Особенности реализации подсистемы безопасности ОС Windows VISTA. 5.5 Особенности реализации подсистемы безопасности ОС Windows 7 5.6. Особенности реализации подсистемы безопасности ОС Windows 8

практическое занятие (8 часа(ов)):

Упражнение 1. Управление учетными записями пользователей и создание групп Упражнение 2. Управление разрешениями в файловой системе NTFS Упражнение 3. Управление локальными политиками безопасности Упражнение 4. Создание и изменение шаблона политики безопасности Упражнение 5. Анализ шаблона политики безопасности Упражнение 6. Настройка подсистемы регистрации и учёта событий

Тема 6. Механизмы защиты информации, реализованные в ОС семейства Linux

лекционное занятие (2 часа(ов)):

6.1 Общий взгляд на архитектуру Linux 6.2. Создание новых пользователей в системе
 6.3. Настройка подсистемы идентификации и аутентификации 6.4. Настройка подсистемы разграничения доступа к файлам 6.5. Настройка подсистемы регистрации и учёта событий 6.6 Настройки безопасности ОС семейства Linux

практическое занятие (8 часа(ов)):

Упражнение 1. Управление учетными записями пользователей и создание групп Упражнение 2. Настройка подсистемы идентификации и аутентификации пользователей Упражнение 3. Установка прав разграничения доступа к файлам Упражнение 4. Настройка подсистемы регистрации и учёта событий

Тема 7. Механизмы защиты информации, реализованные в прикладном программном обеспечении

лекционное занятие (2 часа(ов)):

7.1 Общие положения 7.1 Типы, форматы и размер данных 7.2 Особенности реализации механизмов защиты в СУБД. 7.3 особенности реализации механизмов защиты в серверах приложений

практическое занятие (7 часа(ов)):

Упражнение 1. Управление учетными записями пользователей СУБД Упражнение 2. Настройка подсистемы защиты информации сервера приложений

Тема 8. Механизмы защиты информации, реализованные в активном сетевом оборудовании

лекционное занятие (4 часа(ов)):

8.1. Компоненты корпоративной сети, определяющие уровень безопасности 8.2. Межсетевое экранирование 8.3. Обзор и классификация межсетевых экранов. 8.4. Построение системы обнаружения вторжений 8.5. Проблема эксплуатации защищённых АС, администрирование безопасности информации

практическое занятие (7 часа(ов)):

Упражнение ♦1. Обзор средств разграничения доступа на активном оборудовании
 Упражнение ♦2 Использование средств разграничения доступа на нескольких коммутаторах
 Упражнение ♦3. Создание и удаление виртуальных сетей на коммутаторе Catalyst 2950
 Упражнение ♦4 Конфигурирование средств защиты, встроенных в Cisco IOS

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. Основные вопросы защиты информации | 7 | 1-2 | подготовка к устному опросу | 2 | устный опрос |
| 2. | Тема 2. Уязвимости, угрозы, атаки и их классификации | 7 | 2-3 | подготовка к устному опросу | 2 | устный опрос |
| 3. | Тема 3. Теоретические основы защиты информации | 7 | 4-5 | подготовка к контрольной работе | 8 | контрольная работа |
| 4. | Тема 4. Возможности сканеров уязвимостей | 7 | 6-7 | подготовка к отчету | 4 | отчет |
| 5. | Тема 5. Механизмы защиты информации, реализованные в ОС семейства Windows | 7 | 8-9 | подготовка к отчету | 8 | отчет |
| | | | | подготовка к тестированию | 2 | тестирование |

| N | Раздел Дисциплины | Семестр | Неделя семестра | Виды самостоятельной работы студентов | Трудоемкость (в часах) | Формы контроля самостоятельной работы |
|-------|---|---------|-----------------|---------------------------------------|------------------------|---------------------------------------|
| 6. | Тема 6. Механизмы защиты информации, реализованные в ОС семейства Linux | 7 | 10-13 | подготовка к отчету | 8 | отчет |
| | | | | подготовка к тестированию | 2 | тестирование |
| 7. | Тема 7. Механизмы защиты информации, реализованные в прикладном программном обеспечении | 7 | 14-16 | подготовка к отчету | 5 | отчет |
| | | | | подготовка к тестированию | 5 | тестирование |
| 8. | Тема 8. Механизмы защиты информации, реализованные в активном сетевом оборудовании | 7 | 17-18 | подготовка к контрольной работе | 4 | контрольная работа |
| | | | | подготовка к отчету | 4 | отчет |
| Итого | | | | | 54 | |

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и лабораторных занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки.

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

Тема 1. Основные вопросы защиты информации

устный опрос , примерные вопросы:

? Информация и её свойства ? Автоматизированная система и её ресурсы ? Введение в проблему построения безопасных автоматизированных систем (АС) ? Доступ. Управление доступом

Тема 2. Уязвимости, угрозы, атаки и их классификации

устный опрос , примерные вопросы:

Что такое уязвимости, угрозы безопасности информации в АС, атаки. Какие классификации для них можно выделить

Тема 3. Теоретические основы защиты информации

контрольная работа , примерные вопросы:

дать сравнительные характеристики: понятие однофакторная и многофакторная аутентификация

Тема 4. Возможности сканеров уязвимостей

отчет , примерные вопросы:

? Аудит информационной безопасности и его виды ? Последовательность действий в ходе аудита при помощи сканера ? Обзор методов аудита ИБ, используемых при сканировании ? Структура итогового отчёта

Тема 5. Механизмы защиты информации, реализованные в ОС семейства Windows

отчет , примерные вопросы:

Инсталляция ОС Windows. Настройка подсистемы разграничения доступа. Настройка подсистемы регистрации и учёта. Настройка подсистемы обеспечения целостности. Настройка и использование криптографической подсистемы. Ин-терфейс администратора безопасности. Передача административного контроля. Использование оснасток. Создание антивирусной подсистемы. Построение системы управления обновлениями

тестирование , примерные вопросы:

? Возможности КСЗ ОС семейства Windows ? Подсистема разграничения доступа ? Подсистема регистрации и учёта ? Подсистема обеспечения целостности ? Криптографическая подсистема ? Интерфейс администратора безопасности

Тема 6. Механизмы защиты информации, реализованные в ОС семейства Linux

отчет , примерные вопросы:

Инсталляция ОС Linux. Настройка подсистемы разграничения доступа. Настройка подсистемы регистрации и учёта. Настройка подсистемы обеспечения целостности. Настройка и использование криптографической подсистемы. Системы LIDS и RSBAC.

тестирование , примерные вопросы:

? Возможности комплекса средств защиты (КСЗ) ОС ? Подсистема разграничения доступа ? Подсистема регистрации и учёта ? Подсистема обеспечения целостности ? Криптографическая подсистема ? Интерфейс администратора безопасности

Тема 7. Механизмы защиты информации, реализованные в прикладном программном обеспечении

отчет , примерные вопросы:

Привести результаты настройки механизмов защиты сервера приложения

тестирование , примерные вопросы:

? Подсистема регистрации и учёта ? Подсистема обеспечения целостности ? Криптографическая подсистема ? Интерфейс администратора безопасности

Тема 8. Механизмы защиты информации, реализованные в активном сетевом оборудовании

контрольная работа , примерные вопросы:

обзор механизмов разграничения доступа, реализованных в активном сетевом оборудовании

отчет , примерные вопросы:

Построение малой сети согласно архитектуре Cisco SAFE. Настройка защиты сетевых средств и сервисов. Установка и настройка межсетевых экранов. Установка и настройка системы обнаружения вторжений. Управление системой кодирования информации, передаваемой по открытым каналам связи.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

По данной дисциплине предусмотрено проведение зачета и промежуточных контрольных. Примерные вопросы для зачета - Приложение 1.

Вопрос ♦1:

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. 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

Вопрос ♦2

1. Дайте определения: политика безопасности, профиль защиты, червь.
2. Дайте определение понятий идентификация, аутентификация, авторизация. Опишите механизм. Какие виды аутентификации вы знаете.
3. Дайте определения: задание по безопасности, вирус, объект доступа.
4. Дайте определения: блочный шифр, субъект доступа, автоматизированная система
5. Дайте определения: группа, доступ, межсетевой экран
6. Дайте определения: уязвимость, угроза, атака.
7. Дайте определения: безопасность информации, персонал, КСА
8. Дайте определения: политика безопасности, аудит(все возможные трактовки), пользователи
9. Дайте определения всех видов обеспечения АС

Вопрос ♦3(дополнительный)

1. Проведите сравнение ролевой и дискреционной моделей безопасности, а так же приведите примеры, в каких сферах эти модели могут быть применены.
2. Обзор механизмов криптографической защиты информации
3. Схемы ротации носителей информации.
4. Проведите сравнение ролевой и мандатной моделей безопасности, а так же приведите примеры, в каких сферах эти модели могут быть применены.
5. Проведите сравнение дискреционной и мандатной моделей безопасности, а так же приведите примеры. В каких сферах эти модели могут быть применены.
6. Обзор архитектур систем резервного копирования данных. Какие механизмы вы планируете там использовать и почему.

7.1. Основная литература:

1. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - URL: <http://kpfu.ru/docs/F366166681/mzi.pdf>
2. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013. - 183 с.
<http://znanium.com/catalog.php?bookinfo=415501>
3. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.
<http://znanium.com/catalog.php?bookinfo=423927>

7.2. Дополнительная литература:

1. 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. - ISBN 978-5-369-01178-2

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

2. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-627-0, 1000 экз.

<http://znanium.com/bookread.php?book=420047>

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 "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 оборудование 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 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.

Лекционные занятия по дисциплине проводятся в аудитории, оснащенной проекционным оборудованием. Лабораторные занятия проводятся в специализированных компьютерных кабинетах информатики и вычислительных технологий с выходом в Интернет и установленной интерактивной доской.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 230700.62 "Прикладная информатика" и профилю подготовки не предусмотрено .

Автор(ы):

Иванов К.В. _____

"__" _____ 201__ г.

Рецензент(ы):

Акчурин А.Д. _____

"__" _____ 201__ г.