МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____
"___"_____20___ г.

Программа дисциплины

Безопасность вычислительных систем Б1.В.ДВ.6

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Мубараков Б.Г.
Рецензент(ы):
Ишмухаметов Ш.Т.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Казань
2018

Содержание

Программу дисциплины разработал(а)(и) ассистент, б/с Мубараков Б.Г. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , BGMubarakov@kpfu.ru

1. Цели освоения дисциплины

Цель дисциплины - изучить практические правила управления безопасностью вычислительных систем, научиться применять комплексные подходы к обеспечению безопасности вычислительных систем, научиться анализировать угрозы безопасности, получить навыки анализа рисков безопасности; изучить методы и средства обеспечения безопасности вычислительных систем.

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

Данная учебная дисциплина включена в раздел " Б1.В.ДВ.6 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к дисциплинам по выбору. Осваивается на 3 курсе, 6 семестр.

Данная дисциплина относится к профессиональным дисциплинам. Основывается на знаниях, полученных в рамках дисциплин 'Основы информационной безопасности', 'Теоретические основы компьютерной безопасности'. Знания, полученные в рамках этой дисциплины, понадобятся при изучении других дисциплин профессионального цикла, а также при написании курсовых и выпускных работ.

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-1 (профессиональные компетенции)	способностью анализировать физические явления и процессы для решения профессиональных задач
ОПК-3 (профессиональные компетенции)	способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач
ОПК-4 (профессиональные компетенции)	способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для обработки и поиска информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации
ОПК-7 (профессиональные компетенции)	способностью определять виды информации, виды угроз безопасности информации и возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-1 (профессиональные компетенции)	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-2 (профессиональные компетенции)	способностью принимать участие в эксплуатации подсистем управления информационной безопасностью объекта защиты

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-3 (профессиональные компетенции)	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-4 (профессиональные компетенции)	способностью администрировать подсистемы информационной безопасности объекта защиты

В результате освоения дисциплины студент:

1. должен знать:

- основные требования нормативно-правовой базы информационной безопасности к защите корпоративных информационных систем и их компонентов от несанкционированного доступа к информации

2. должен уметь:

- уметь использовать методы выявления причин, видов, источников и каналов утечки, информации.
- уметь выявлять категории атак на вычислительные системы

3. должен владеть:

- навыками формирования требований к средствам защиты информации

4. должен демонстрировать способность и готовность:

- применять полученные знания в своей профессиональной деятельности

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет в 6 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. Вычислительные системы. Информационная безопасность вычислительных систем, основные понятия и определения, методологии безопасности	6	1-3	3	0	3	Письменное домашнее задание
2.	Тема 2. Организационно-методологические основы анализа информационной безопасности вычислительных систем	6	4-6	3	0	3	Письменное домашнее задание Контрольная работа
3.	Тема 3. Нормативно-правовая база информационной безопасности вычислительных систем	6	7-9	3	0	3	Письменное домашнее задание
4.	Тема 4. Виды атак на вычислительные системы. Обнаружение вторжений.	6	10-12	3	0	3	
5.	Тема 5. Криптографические методы защиты информации.	6	13-15	3	0	3	Лабораторные работы
6.	Тема 6. Применение криптографических методов защиты информации в вычислительных системах	6	16-18	3	0	3	Контрольная работа Лабораторные работы
.	Тема . Итоговая форма контроля	6		0	0	0	Зачет
	Итого			18	0	18	

4.2 Содержание дисциплины

Тема 1. Введение. Вычислительные системы. Информационная безопасность вычислительных систем, основные понятия и определения, методологии безопасности

лекционное занятие (3 часа(ов)):

Основные понятия и определения. Современное состояние и перспективы развития защиты информации

лабораторная работа (3 часа(ов)):

Разбираются практические примеры для понимания понятия защиты информации.

Тема 2. Организационно-методологические основы анализа информационной безопасности вычислительных систем

лекционное занятие (3 часа(ов)):

Принципы организации системы защиты, политика информационной безопасности, направления, способы и методы защиты.

лабораторная работа (3 часа(ов)):

Рассматриваются основные методы анализа рисков информационной безопасности. Методология CORAS, матричный подход и т.д.

Тема 3. Нормативно-правовая база информационной безопасности вычислительных систем

лекционное занятие (3 часа(ов)):

Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности. Международные правовые акты по защите информации.

лабораторная работа (3 часа(ов)):

Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций. Виды тайн и законодательство по ограничениям оборота информации, относимой к различным тайнам

Тема 4. Виды атак на вычислительные системы. Обнаружение вторжений.

лекционное занятие (3 часа(ов)):

Рассматриваются основные виды атак. Проводится детальное рассмотрение каждой из атак и способы защиты.

лабораторная работа (3 часа(ов)):

Проводится детальное рассмотрение каждой из атак и способы защиты.

Тема 5. Криптографические методы защиты информации.

лекционное занятие (3 часа(ов)):

Рассматриваются основные принципы, подходы и методы современной криптографии. Криптосистемы с секретными и открытыми ключами, криптографические хэш-функции, методы электронной подписи, криптосистемы на эллиптических кривых.

лабораторная работа (3 часа(ов)):

Рассматриваются алгоритмы криптографических методов и средств защиты информации для обеспечения конфиденциальности, подтверждения целостности, аутентификации.

Тема 6. Применение криптографических методов защиты информации в вычислительных системах

лекционное занятие (3 часа(ов)):

Рассматриваются основные принципы, подходы и методы современной криптографии. Криптосистемы с секретными и открытыми ключами, криптографические хэш-функции, методы электронной подписи, криптосистемы на эллиптических кривых.

лабораторная работа (3 часа(ов)):

Рассматриваются алгоритмы криптографических методов и средств защиты информации для обеспечения конфиденциальности, подтверждения целостности, аутентификации.

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. Вычислительные системы. Информационная безопасность вычислительных систем, основные понятия и определения, методологии безопасности	6	1-3	подготовка домашнего задания	4	домашнее задание
2.	Тема 2. Организационно-методологические основы анализа информационной безопасности вычислительных систем	6	4-6	подготовка домашнего задания	8	домашнее задание
				подготовка к контрольной работе	4	контрольная работа
3.	Тема 3. Нормативно-правовая база информационной безопасности вычислительных систем	6	7-9	подготовка домашнего задания	4	домашнее задание
5.	Тема 5. Криптографические методы защиты информации.	6	13-15	выполнение лабораторной работы	4	Лабораторные работы
6.	Тема 6. Применение криптографических методов защиты информации в вычислительных системах	6	16-18	выполнение лабораторной работы	4	Лабораторные работы
				подготовка к контрольной работе	8	контрольная работа
	Итого				36	

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 экзамена минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов дисциплины 'Безопасность вычислительных систем' на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные 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 к зачету, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени.

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

Тема 1. Введение. Вычислительные системы. Информационная безопасность вычислительных систем, основные понятия и определения, методологии безопасности

домашнее задание , примерные вопросы:

Выучить основные определения и понятия информационной безопасности

Тема 2. Организационно-методологические основы анализа информационной безопасности вычислительных систем

домашнее задание , примерные вопросы:

Изучить организационно-методологические основы анализа информационной безопасности вычислительных систем

контрольная работа , примерные вопросы:

Вариант 1. Управление рисками. Модель безопасности с полным перекрытием Вариант 2. Методики и программные продукты для оценки рисков

Тема 3. Нормативно-правовая база информационной безопасности вычислительных систем

домашнее задание , примерные вопросы:

Изучить нормативно-правовую базу информационной безопасности вычислительных систем.

Тема 4. Виды атак на вычислительные системы. Обнаружение вторжений.

Тема 5. Криптографические методы защиты информации.

Лабораторные работы , примерные вопросы:

Реализация простейших алгоритмов шифрования с закрытым ключом. Шифр Цезаря, Виженера.

Тема 6. Применение криптографических методов защиты информации в вычислительных системах

контрольная работа , примерные вопросы:

Задачи по факторизации натуральных чисел без использования компьютера.

Лабораторные работы , примерные вопросы:

Реализация алгоритма RSA.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

1.Концепции и аспекты обеспечения информационной безопасности
2.Виды угроз информационной безопасности
3.Основы законодательства в области обеспечения информационной безопасности
4.Построения системы информационной безопасности
5.Категории атак
6.Управление риском
7.Обнаружение вторжений

8.Алгоритмы симметричного метода шифрования
9.Алгоритмы асимметричного метода шифрования

7.1. Основная литература:

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

2. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. URL:http://znanium.com/bookread2.php?book=495249

3. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие. - Электрон. дан. - СПб. : Лань, 2016. - 324 с. - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=75515

4. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. - 118 с. http://znanium.com/bookread2.php?book=507334

7.2. Дополнительная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=491597

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

3. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. URL: http://znanium.com/bookread.php?book=335362

4. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с. ЭБС 'Знаниум': http://znanium.com/bookread2.php?book=50838

7.3. Интернет-ресурсы:

Интернет-портал с образовательными ресурсами по ИТ - http://www.intuit.ru
Компьютерная энциклопеция - http://www.computer-encyclopedia.ru/main.php?n=2&f=14
Научная электронная библиотека - https://elibrary.ru
Официальный сайт ФСТЭК России - http://www.fstec.ru
Справочная система MSDN - http://msdn.com

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Безопасность вычислительных систем" 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.

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.

Лекции по дисциплине проводятся в аудитории, оснащенной проектором, практические занятия по дисциплине проходят в компьютерном классе.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность компьютерных систем .

Автор(ы):
Мубараков Б.Г. _____
"__" _____ 201 __ г.

Рецензент(ы):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.