МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Набережночелнинский институт (филиал)
Отделение информационных технологий и энергетических систем

Утверждаю

Первый заместитель директора
НЧИ КФУ Симонова Л. А.

"__" _____ 20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Безопасность информационных систем Б1.В.01

Направление подготовки: 09.04.01 - Информатика и вычислительная техника
Профиль подготовки: Автоматизированные системы обработки информации и управления
Квалификация выпускника: магистр
Форма обучения: заочное
Язык обучения: русский
Год начала обучения по образовательной программе: 2019
Автор(ы): Хазиев Э.Л.
Рецензент(ы): Балабанов И.П.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Валиев Р. А.
Протокол заседания кафедры No ___ от "____" _____ 20__г.
Учебно-методическая комиссия Высшей инженерной школы (Отделение информационных технологий и энергетических систем) (Набережночелнинский институт (филиал)):
Протокол заседания УМК No ____ от "____" _____ 20__г.

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. Хазиев Э.Л. (Кафедра информационных систем НИ, Отделение информационных технологий и энергетических систем), ELHaziev@kpfu.ru

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Выпускник, освоивший дисциплину, должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-3	Способен управлять развитием инфокоммуникационной системы организации

Выпускник, освоивший дисциплину:

Должен знать:

- методы и средства обеспечения информационной безопасности компьютерных систем

Должен уметь:

- выбирать, комплексировать и эксплуатировать программно-аппаратные средства в создаваемых вычислительных и информационных системах и сетевых структурах;

- ставить задачу и разрабатывать алгоритм ее решения, использовать прикладные системы программирования, разрабатывать основные программные документы

Должен владеть:

- языками процедурного и объектно-ориентированного программирования, навыками разработки и отладки программ не менее чем на одном из алгоритмических процедурных языков программирования высокого уровня

Должен демонстрировать способность и готовность:

- применять результаты обучения по дисциплине в профессиональной деятельности.

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

Данная учебная дисциплина включена в раздел "Б1.В.01 Дисциплины (модули)" основной профессиональной образовательной программы 09.04.01 "Информатика и вычислительная техника (Автоматизированные системы обработки информации и управления)" и относится к вариативной части.
Осваивается на 1 курсе в 1, 2 семестрах.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) на 144 часа(ов).

Контактная работа - 10 часа(ов), в том числе лекции - 4 часа(ов), практические занятия - 2 часа(ов), лабораторные работы - 4 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 130 часа(ов).

Контроль (зачёт / экзамен) - 4 часа(ов).

Форма промежуточного контроля дисциплины: отсутствует в 1 семестре; зачет во 2 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Правовое обеспечение информационной безопасности	1	0	0	0	2
2.	Тема 2. Основы информационной безопасности	1	1	0	0	6

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Безопасность операционных систем	1	0	0	1	8
4.	Тема 4. Безопасность вычислительных сетей	1	0	0	1	8
5.	Тема 5. Безопасность систем управления базами данных	1	1	0	0	8
6.	Тема 6. Организационное обеспечение информационной безопасности	2	0	0	0	16
7.	Тема 7. Программно-аппаратные средства защиты информации	2	0	0	0	16
8.	Тема 8. Криптографические методы защиты информации	2	0	0	0	39
9.	Тема 9. Комплексное обеспечение информационной безопасности автоматизированных систем	2	2	2	2	27
	Итого		4	2	4	130

4.2 Содержание дисциплины

Тема 1. Правовое обеспечение информационной безопасности

Конституционные гарантии прав граждан на информацию и механизмы их реализации. Понятие и виды защищаемой информации по законодательству РФ. Системы защиты государственной тайны и конфиденциальной информации. Лицензирование и сертификация в области защиты государственной тайны и конфиденциальной информации. Защита интеллектуальной собственности. Преступления в сфере компьютерной информации.

Организационно-правовое обеспечение защиты компьютерной информации.

Изучение системы защиты конфиденциальной информации. Модели информационной безопасности; международные и отечественные стандарты информационной безопасности, политика безопасности; показатели защищенности средств вычислительной техники и классы защищенности автоматизированных систем от несанкционированного доступа.

Тема 2. Основы информационной безопасности

Понятие национальной безопасности Российской Федерации. Информационная безопасность (ИБ) в системе национальной безопасности РФ, проблемы информационной войны. Основные понятия, общеметодологические принципы теории ИБ. Модели информационной безопасности; международные и отечественные стандарты информационной безопасности, политика безопасности; показатели защищенности средств вычислительной техники и классы защищенности автоматизированных систем от несанкционированного доступа. Угрозы ИБ. Оценка и управление рисками. Обеспечение конфиденциальности, целостности и доступности информации.

Обеспечение безопасности электронной почты при работе в сети Интернет.

Отработка безопасных механизмов работы с почтой в сети Интернет.

Тема 3. Безопасность операционных систем

Общая характеристика операционных систем. Назначение, возможности, модели безопасности операционных систем группы Windows, NetWare, клона UNIX. Организация управления доступом и защиты ресурсов ОС. Основные механизмы безопасности: средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС.

Безопасность операционных систем.

Изучение основных механизмов безопасности ОС: средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита.

Тема 4. Безопасность вычислительных сетей

Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Интеграция локальных вычислительных сетей в глобальные. Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Протоколы аутентификации Kerberos, SSL, TLS. Технология PKI (Public Key Infrastructure) ? интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих шифрование с открытым ключом, а также для управления ими. Многоуровневая защита корпоративных сетей. Виртуальные частные сети, варианты построения и продукты реализации. Режим функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Системы адаптивного анализа защищенности. Задачи и программно-аппаратные средства администратора безопасности сети.

Использование межсетевых экранов при работе в локальной вычислительной сети предприятия и сети Интернет.

Изучение принципов работы и возможностей программных средств обеспечения сетевой безопасности.

Тема 5. Безопасность систем управления базами данных

Методы и средства идентификации и аутентификации пользователей СУБД, системные и объектные привилегии, разграничение прав на выполнение операций над объектами баз данных, средства языка SQL для организации разграничения доступа, концепция и реализация механизма ролей, использование представлений, организация аудита системных событий и действий пользователя в системах баз данных. Триггеры и их применение в базах данных. Обеспечение непротиворечивости, транзакции. Использование блокировок. Ограничения ссылочной целостности баз данных. Организация взаимодействия СУБД и базовой ОС, журнализация, методы и средства создания резервных копий и восстановления баз данных. Защита баз данных от аппаратных и программных сбоев. Обеспечение безопасности доступа к базам данных в технологии клиент/сервер. Задачи и программно-аппаратные средства администратора безопасности баз данных.

Безопасность систем управления базами данных.

Изучение взаимодействия СУБД и базовой ОС, журнализация, методы и средства создания резервных копий и восстановления баз данных. Защита баз данных от аппаратных и программных сбоев. Обеспечение безопасности доступа к базам данных в технологии клиент/сервер. Задачи и программно-аппаратные средства администратора безопасности баз данных.

Тема 6. Организационное обеспечение информационной безопасности

Исходная концептуальная схема (парадигма) обеспечения информационной безопасности (ИБ) организации. Общие и специальные принципы обеспечения ИБ организации. Модели угроз и нарушителей информационной безопасности организации.

Политика ИБ организации: состав, назначение, общие требования по обеспечению ИБ, отображаемые в политике ИБ организации; общие требования по обеспечению ИБ при распределении ролей и обеспечении доверия к персоналу; общие требования по обеспечению ИБ автоматизированных систем на стадиях жизненного цикла; общие требования по обеспечению ИБ при управлении доступом и регистрации; общие требования по обеспечению ИБ средствами антивирусной защиты; общие требования по обеспечению ИБ при использовании ресурсов сети Интернет; общие требования по обеспечению ИБ при использовании средств криптографической защиты информации.

Система менеджмента ИБ организации: планирование; реализация и эксплуатация СМИБ; проверка (мониторинг и анализ) СМИБ; совершенствование СМИБ; система документации; обеспечение непрерывности деятельности и восстановление после прерываний; служба информационной безопасности организации.

Проверка и оценка информационной безопасности организации. Модель зрелости процессов менеджмента информационной безопасности организации.

Программно-аппаратные средства защиты компьютерной информации от НСД.

Изучение назначения и принципов создания программно-аппаратных средств обеспечения информационной безопасности. Типовая структура комплексной системы защиты информации от НСД.

Тема 7. Программно-аппаратные средства защиты информации

Назначение и принципы создания программно-аппаратных средств обеспечения информационной безопасности. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, принципы их действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем. Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации. Защита программ от изучения, способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий, защита программ от изменения и контроль целостности, построение изолированной программной среды. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям безопасности информации. Основные категории требований к программно-аппаратной реализации средств обеспечения информационной безопасности. Программно-аппаратные средства защиты информации в сетях передачи данных.

Инфраструктура открытого ключа в Windows 2003 и ее применение в различных приложениях.

Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС.

Тема 8. Криптографические методы защиты информации

Моноалфавитные и полиалфавитные шифры. Блочные и потоковые шифры. Симметричные криптосистемы. Стандарты шифрования данных DES, Triple-DES, AES и основные режимы их работы. Отечественный стандарт ГОСТ 28147-89 и режимы его работы.

Асимметричные криптосистемы. Однонаправленные функции. Криптосистема RSA, ее безопасность и быстродействие. Схема шифрования Полига-Хеллмана. Схема шифрования Эль-Гамаля. Комбинированный метод шифрования.

Идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей. Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Алгоритм хэширования SHA-1. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции ГОСТ Р.34.11-94. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р34.10-94.

Реализация блочных шифров 3DES, CAST и IDEA, а также поддержка алгоритм хэширования SHA-1 для вычисления цифровой подписи в пакете PGP. Российские разработки: ?Верба?, ?Криптон?, ?Крипто-Про?, ?Лан-Крипто? и др.

Асимметричное шифрование. Электронно-цифровая подпись.

Изучение криптографических методов защиты информации. Идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей. Проблема аутентификации данных и электронная цифровая подпись.

Тема 9. Комплексное обеспечение информационной безопасности автоматизированных систем

Постановка проблемы комплексного обеспечения ИБ автоматизированных систем. Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), методология формирования задач защиты. Этапы проектирования КСИБ и требования к ним: предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение. Типовая структура комплексной системы защиты информации от НСД. Методика выявления возможных каналов НСД, последовательность работ при проектировании КСИБ, моделирование как инструментарий проектирования. Методы оценки качества КСИБ. Требования к эксплуатационной документации КСИБ, аттестация по требованиям безопасности информации.

Методы выявления каналов НСД.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301).

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений".

Положение от 29 декабря 2018 г. № 0.1.1.67-08/328 "О порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет".

Положение № 0.1.1.67-06/241/15 от 14 декабря 2015 г. "О формировании фонда оценочных средств для проведения текущей, промежуточной и итоговой аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет"".

Положение № 0.1.1.56-06/54/11 от 26 октября 2011 г. "Об электронных образовательных ресурсах федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"".

Регламент № 0.1.1.67-06/66/16 от 30 марта 2016 г. "Разработки, регистрации, подготовки к использованию в учебном процессе и удаления электронных образовательных ресурсов в системе электронного обучения федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет"".

Регламент № 0.1.1.67-06/11/16 от 25 января 2016 г. "О балльно-рейтинговой системе оценки знаний обучающихся в федеральном государственном автономном образовательном учреждении высшего образования "Казанский (Приволжский) федеральный университет"".

Регламент № 0.1.1.67-06/91/13 от 21 июня 2013 г. "О порядке разработки и выпуска учебных изданий в федеральном государственном автономном образовательном учреждении высшего профессионального образования "Казанский (Приволжский) федеральный университет"".

6. Фонд оценочных средств по дисциплине (модулю)

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
Семестр 1			
	Текущий контроль		
1	Тестирование	ПК-3	1. Правовое обеспечение информационной безопасности 2. Основы информационной безопасности 3. Безопасность операционных систем 4. Безопасность вычислительных сетей 5. Безопасность систем управления базами данных
2	Лабораторные работы	ПК-3	3. Безопасность операционных систем 4. Безопасность вычислительных сетей
Семестр 2			
	Текущий контроль		
1	Тестирование	ПК-3	6. Организационное обеспечение информационной безопасности 7. Программно-аппаратные средства защиты информации 8. Криптографические методы защиты информации 9. Комплексное обеспечение информационной безопасности автоматизированных систем
2	Лабораторные работы	ПК-3	9. Комплексное обеспечение информационной безопасности автоматизированных систем
3	Реферат	ПК-3	9. Комплексное обеспечение информационной безопасности автоматизированных систем
	Зачет	ПК-3	

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Семестр 1					
Текущий контроль					
Тестирование	86% правильных ответов и более.	От 71% до 85 % правильных ответов.	От 56% до 70% правильных ответов.	55% правильных ответов и менее.	1
Лабораторные работы	Оборудование и методы использованы правильно. Проявлена превосходная теоретическая подготовка. Необходимые навыки и умения полностью освоены. Результат лабораторной работы полностью соответствует её целям.	Оборудование и методы использованы в основном правильно. Проявлена хорошая теоретическая подготовка. Необходимые навыки и умения в основном освоены. Результат лабораторной работы в основном соответствует её целям.	Оборудование и методы частично использованы правильно. Проявлена удовлетворительная теоретическая подготовка. Необходимые навыки и умения частично освоены. Результат лабораторной работы частично соответствует её целям.	Оборудование и методы использованы неправильно. Проявлена неудовлетворительная теоретическая подготовка. Необходимые навыки и умения не освоены. Результат лабораторной работы не соответствует её целям.	2
Семестр 2					
Текущий контроль					
Тестирование	86% правильных ответов и более.	От 71% до 85 % правильных ответов.	От 56% до 70% правильных ответов.	55% правильных ответов и менее.	1

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Лабораторные работы	Оборудование и методы использованы правильно. Проявлена превосходная теоретическая подготовка. Необходимые навыки и умения полностью освоены. Результат лабораторной работы полностью соответствует её целям.	Оборудование и методы использованы в основном правильно. Проявлена хорошая теоретическая подготовка. Необходимые навыки и умения в основном освоены. Результат лабораторной работы в основном соответствует её целям.	Оборудование и методы частично использованы правильно. Проявлена удовлетворительная теоретическая подготовка. Необходимые навыки и умения частично освоены. Результат лабораторной работы частично соответствует её целям.	Оборудование и методы использованы неправильно. Проявлена неудовлетворительная теоретическая подготовка. Необходимые навыки и умения не освоены. Результат лабораторной работы не соответствует её целям.	2
Реферат	Тема раскрыта полностью. Продемонстрировано превосходное владение материалом. Использованы надлежащие источники в нужном количестве. Структура работы соответствует поставленным задачам. Степень самостоятельности работы высокая.	Тема в основном раскрыта. Продемонстрировано хорошее владение материалом. Использованы надлежащие источники. Структура работы в основном соответствует поставленным задачам. Степень самостоятельности работы средняя.	Тема раскрыта слабо. Продемонстрировано удовлетворительное владение материалом. Использованные источники и структура работы частично соответствуют поставленным задачам. Степень самостоятельности работы низкая.	Тема не раскрыта. Продемонстрировано неудовлетворительное владение материалом. Использованные источники недостаточны. Структура работы не соответствует поставленным задачам. Работа несамостоятельна.	3
	Зачтено		**Не зачтено**		
Зачет	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных программой дисциплины.		Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.		

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Семестр 1

Текущий контроль

1. Тестирование

Темы 1, 2, 3, 4, 5

Тема 1. Правовое обеспечение информационной безопасности.

1) Какой федеральный закон регулирует отношения в сфере защиты компьютерной информации?

Федеральный закон от 7.07.2004г. №122-а4 ?О защите информации?.

Федеральный закон от 27.07.2006г. №149-ф3 ?Об информации, информационных технологиях и о защите информации?.

Федеральный закон от 21.05.2002г. №35-г13 ?Информационные технологии и о защита информации в автоматизированных информационных системах?.

2) Назовите правовое основание процесса лицензирования и сертификации в области защиты государственной тайны и конфиденциальной информации.

Постановление Правительства Российской Федерации от3.03.2002г. ?О лицензировании деятельности по разработке и производству средств защиты в области защиты государственной тайны?.

Постановление Правительства Российской Федерации от 3.03.2012г. ?О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации?.

Постановление Правительства Российской Федерации от 13.02.2010г. ?О лицензировании деятельности по разработке средств защиты конфиденциальной информации?.

Тема 2. Основы информационной безопасности.

1) Какое количество уровней содержится в системе защиты от угроз нарушения конфиденциальности информации?

5, 6, 7

2) Идентификация ? это ?

присвоение субъектам доступа уникальных идентификаторов;

присвоение субъектам доступа определенных прав доступа;

проверка принадлежности субъекту доступа предъявленного им идентификатора.

Тема 3. Безопасность операционных систем.

1) Что представляет из себя сертификат операционной системы?

шестнадцатеричную подпись, связывающую значение общего ключа с идентификацией человека, устройства или сервиса, который содержит соответствующий личный ключ;

восьмеричную подпись, связывающую значение общего ключа с идентификацией человека, устройства или сервиса, который содержит соответствующий личный ключ;

двоичную подпись, связывающую значение общего ключа с идентификацией человека, устройства или сервиса, который содержит соответствующий личный ключ.

2) На чем основан механизм аутентификации с синхронизацией по времени?

на значении определенного промежутка времени; на алгоритме, который через определенный интервал времени генерирует случайное число; на схеме с использованием слова-вызова.

Тема 4. Безопасность вычислительных сетей.

1) Назовите криптографический пакет, используемый для шифрования.

OpenSSL; OpenRSA; OpenDSA.

2) Kerberos ? это?

сетевая служба, предназначенная для централизованного решения задач аутентификации и авторизации в крупных сетях; алгоритм шифрования на основе открытых ключей; симметричный алгоритм шифрования.

Тема 5. Безопасность систем управления базами данных.

1) Какой тип технологии шифрования не поддерживает SQL Server 2008?

расширенное управление ключами - Extensible Key Management (EKM);

прозрачное шифрование данных ? Transparent Data Encryption (TDE);

закрытое шифрование данных - Closed Data Encryption (CDE).

2) Используя какой протокол можно обеспечить безопасную передачу данных с клиента на сервер?

SSL/SSH; SSR/SSH; SSK/SSH

Тест для проверки остаточных знаний.

1. Под информационной безопасностью понимается?

А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия

В) нет правильного ответа

2. Защита информации ? это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность ? это?

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

6. Целостность ? это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

7. Конфиденциальность ? это..
А) защита от несанкционированного доступа к информации
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур
8. Для чего создаются информационные системы?
А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные
9. Целостность можно подразделить:
А) статическую
Б) динамичную
В) структурную
10. Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений
11. Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) все ответы правильные
12. Угроза ? это?
А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа
13. Атака ? это?
А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.
14. Источник угрозы ? это..
А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа
15. Окно опасности ? это?
А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере
16. Какие события должны произойти за время существования окна опасности?
А) должно стать известно о средствах использования пробелов в защите.
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.
17. Угрозы можно классифицировать по нескольким критериям:
А) по спектру И.Б.
Б) по способу осуществления
В) по компонентам И.С.
17. По каким компонентам классифицируется угрозы доступности:
А) отказ пользователей
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе
18. Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) все ответы правильные
19. Основными источниками внутренних отказов являются:
А) ошибки при конфигурировании системы
Б) отказы программного или аппаратного обеспечения

В) выход системы из штатного режима эксплуатации

20. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности

Б) обрабатывать большой объем программной информации

В) нет правильного ответа

21Какие существуют грани вредоносного П.О.?

А) вредоносная функция

Б) внешнее представление

В) способ распространения

22. По механизму распространения П.О. различают:

А) вирусы

Б) черви

В) все ответы правильные

23 Вирус ? это?

А) код обладающий способностью к распространению путем внедрения в другие программы

Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов

В) небольшая программа для выполнения определенной задачи

24 Черви ? это?

А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения

Б) код обладающий способностью к распространению путем внедрения в другие программы

В) программа действий над объектом или его свойствами

2. Лабораторные работы

Темы 3, 4

1) Организационно-правовое обеспечение защиты компьютерной информации.

Изучение системы защиты конфиденциальной информации. Модели информационной безопасности; международные и отечественные стандарты информационной безопасности, политика безопасности; показатели защищенности средств вычислительной техники и классы защищенности автоматизированных систем от несанкционированного доступа.

2) Обеспечение безопасности электронной почты при работе в сети Интернет.

Отработка безопасных механизмов работы с почтой в сети Интернет.

3) Безопасность операционных систем.

Изучение основных механизмов безопасности ОС: средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита.

4) Использование межсетевых экранов при работе в локальной вычислительной сети предприятия и сети Интернет.

Изучение принципов работы и возможностей программных средств обеспечения сетевой безопасности.

5) Безопасность систем управления базами данных.

Изучение взаимодействия СУБД и базовой ОС, журнализация, методы и средства создания резервных копий и восстановления баз данных. Защита баз данных от аппаратных и программных сбоев. Обеспечение безопасности доступа к базам данных в технологии клиент/сервер. Задачи и программно-аппаратные средства администратора безопасности баз данных.

6) Настройка брандмауэра. Межсетевого экрана локальной сети

7) Шифрование данных при передаче данных в локальной сети. Генерация сертификатов с использованием Let's Encrypt в ОС Linux.

8) Усиление процесса аутентификации в ОС Linux.

9) Контроль за объектами файловой системы с помощью SELinux. Установка и активация SELinux. Применение политик SELinux.

10) Системные группы и принцип наименьших привилегий. Изоляция процессов в контейнерах. Сканирование на наличие опасных идентификаторов пользователей. Аудит системных ресурсов. Сканирование на наличие открытых портов. Сканирование на предмет активных служб.

Семестр 2

Текущий контроль

1. Тестирование

Темы 6, 7, 8, 9

Тема 6. Организационное обеспечение информационной безопасности.

1) Что нельзя отнести к организационным мерам и мерам обеспечения физической безопасности?

служба охраны и физической безопасности;

регламентация порядка работы с носителями, содержащими конфиденциальную информацию;

парольная система аутентификации.
2) В число классов требований доверия безопасности "Общих критериев" входят: (2 варианта ответа)
разработка; оценка профиля защиты; сертификация

Тема 7. Программно-аппаратные средства защиты информации.
1) Назовите российскую разработку по генерации открытых ключей.
Лан-шифр, Вектор, КриптоПро
2) Назовите систему предотвращения вторжений
IDS; IPS; IRS

Тема 8. Криптографические методы защиты информации.
1) Какой алгоритм является устаревшим и не используемым в настоящее время?
DES, AES, DSA
2) Какой алгоритм используется для шифрования данных в системе мобильной цифровой связи?
A3; A4; A5.

Тема 9. Комплексное обеспечение информационной безопасности автоматизированных систем.
1) Назовите элемент системы защиты внешнего периметра автоматизированной системы.
DIS, IPS, EFS
2) Политика безопасности строится на основе:
общих представлений об ИС организации; изучения политик родственных организаций; анализа рисков.

Тест для проверки остаточных знаний
25 Конфиденциальную информацию можно разделить:
А) предметную
Б) служебную
В) глобальную

26 Природа происхождения угроз:
А) случайные
Б) преднамеренные
В) природные

27 Предпосылки появления угроз:
А) объективные
Б) субъективные
В) преднамеренные

28 К какому виду угроз относится присвоение чужого права?
А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

29 Отказ, ошибки, сбой ? это:
А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

30 Отказ - это?
А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

31 Ошибка ? это?
А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

32 Сбой ? это?
А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

33 Побочное влияние ? это?
А) негативное воздействие на систему в целом или отдельные элементы
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

34 СЗИ (система защиты информации) делится:

А) ресурсы автоматизированных систем

Б) организационно-правовое обеспечение

В) человеческий компонент

35 Что относится к человеческому компоненту СЗИ?

А) системные порты

Б) администрация

В) программное обеспечение

36 Что относится к ресурсам А.С. СЗИ?

А) лингвистическое обеспечение

Б) техническое обеспечение

В) все ответы правильные

37 По уровню обеспеченной защиты все системы делят:

А) сильной защиты

Б) особой защиты

В) слабой защиты

38 По активности реагирования СЗИ системы делят:

А) пассивные

Б) активные

В) полупассивные

39 Правовое обеспечение безопасности информации ? это?

А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) нет правильного ответа

40 Правовое обеспечение безопасности информации делится:

А) международно-правовые нормы

Б) национально-правовые нормы

В) все ответы правильные

41 Информацию с ограниченным доступом делят:

А) государственную тайну

Б) конфиденциальную информацию

В) достоверную информацию

42 Что относится к государственной тайне?

А) сведения, защищаемые государством в области военной, экономической ? деятельности

Б) документированная информация

В) нет правильного ответа

43 Вредоносная программа - это?

А) программа, специально разработанная для нарушения нормального функционирования систем

Б) упорядочение абстракций, расположение их по уровням

В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

44 Основополагающие документы для обеспечения безопасности внутри организации:

А) трудовой договор сотрудников

Б) должностные обязанности руководителей

В) коллективный договор

45 К организационно - административному обеспечению информации относится:

А) взаимоотношения исполнителей

Б) подбор персонала

В) регламентация производственной деятельности

46 Что относится к организационным мероприятиям:

А) хранение документов

Б) проведение тестирования средств защиты информации

В) пропускной режим

47 Какие средства используется на инженерных и технических мероприятиях в защите информации:

А) аппаратные

Б) криптографические

В) физические

48 Программные средства ? это?

А) специальные программы и системы защиты информации в информационных системах различного назначения

Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла

В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

49 . Криптографические средства ? это?

А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования

Б) специальные программы и системы защиты информации в информационных системах различного назначения

В) механизм, позволяющий получить новый класс на основе существующего

2. Лабораторные работы

Тема 9

1) Программно-аппаратные средства защиты компьютерной информации от НСД.

Изучение назначения и принципов создания программно-аппаратных средств обеспечения информационной безопасности. Типовая структура комплексной системы защиты информации от НСД.

2) Инфраструктура открытого ключа в Windows 2003 и ее применение в различных приложениях.

Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС.

3) Асимметричное шифрование. Электронно-цифровая подпись.

Изучение криптографических методов защиты информации. Идентификация и аутентификация пользователя. Взаимная проверка подлинности пользователей. Проблема аутентификации данных и электронная цифровая подпись.

4) Методы выявления каналов НСД.

Изучение методик выявления каналов утечки и несанкционированного доступа к информационным ресурсам.

5) Поиск установленного программного обеспечения в Linux.

6) Создание туннеля OpenVPN. Конфигурирование сервера OpenVPN.

7) Конфигурирование клиента OpenVPN. Тестирование VPN.

8) Построение сетей, защищенных от вторжений. Демилитаризованные зоны (DMZ). Использование iptables. Создание DMZ с помощью iptables. Создание DMZ с помощью Shorewall.

9) Построение виртуальной сети для тестирования инфраструктуры.

10) Работа с системными журналами.

3. Реферат

Тема 9

1. Настройка безопасности ОС Windows при работе в сети
2. Организация антивирусной защиты частного предприятия
3. Криптографические системы защиты данных
4. Компьютерная преступность и компьютерная безопасность
5. Ответственность за нарушения в сфере информационного права
6. Комплекс технических решений по защите информации, записанной на отчуждаемых электронных носителях
7. Защита почтовых сообщений
8. Защита баз данных
9. Защита цифровой информации методами стеганографии
10. Криптология: подстановочно-перестановочный шифр и его применение
11. Информация и личная безопасность
12. Защита информации в ПЭВМ. Шифр Плейфера
13. Защита информации от несанкционированного доступа методом криптопреобразования Обеспечение информационной безопасности в сети Internet
14. Источники возникновения и последствия реализации угроз информационной безопасности
15. Российский рынок информационной безопасности
16. Системы распределения прав (Rights Management Systems)
17. Решение современных проблем информационной безопасности корпоративных вычислительных сетей
18. Спам и нормы пользования сетью
19. Защита информации в глобальной сети
20. Системы обнаружения атак. (Анализаторы сетевых протоколов и сетевые мониторы) Криптология: точки соприкосновения математики и языкознания
21. Каналы утечки информации
22. Преступления в сфере компьютерной информации
23. Компьютерная преступность и компьютерная безопасность

Зачет

Вопросы к зачету:

1. Информационная безопасность. Базовые свойства защищаемой информации.
2. Методы обеспечения информационной безопасности.
3. Угрозы информационной безопасности. Классификация угроз. Методы перечисления угроз.
4. Структура системы защиты от угроз нарушения конфиденциальности информации.
5. Организационные меры и меры обеспечения физической безопасности.
6. Идентификация и аутентификация. Базовая схема идентификации и аутентификации.
7. Методы аутентификации.
8. Особенности парольных систем аутентификации. Основные угрозы безопасности парольных систем.
9. Основные рекомендации при практической реализации парольных систем.
10. Методы хранения паролей. Передача паролей по сети.
11. Разграничение доступа. Дискреционный и мандатный методы разграничения доступа. Матрица доступа.
12. Разграничение доступа. Ролевое управление доступом.
13. Криптографические методы обеспечения конфиденциальности информации.
14. Защита внешнего периметра. Межсетевое экранирование.
15. Защита внешнего периметра. Системы обнаружения вторжений(IDS).
16. Защита внешнего периметра. Системы предотвращения вторжений(IPS).
17. Протоколирование и аудит.
18. Каналы утечки информации технических средств обработки, хранения и передачи информации.
19. Каналы утечки речевой информации.
20. Каналы утечки информации при её передаче по каналам связи.
21. Технические каналы утечки видовой информации.
22. Каналы утечки информации, создаваемые атаками извне и внутри корпоративных систем ИКТ (объекта информатизации).
23. Принципы обеспечения целостности информации.
24. Криптографические методы обеспечения целостности информации. Цифровые подписи.
25. Криптографические методы обеспечения целостности информации. Криптографические хэш-функции.
26. Криптографические методы обеспечения целостности информации. Коды проверки подлинности.
27. Криптографические методы обеспечения целостности информации. Технология Blockchain.
28. Построение систем защиты от угроз нарушения доступности. Получение информации. Дублирование каналов связи, дублирование шлюзов и межсетевых экранов.
29. Построение систем защиты от угроз нарушения доступности. Обработка информации. Дублирование серверов. Использование кластеров.
30. Построение систем защиты от угроз нарушения доступности. Хранение информации. Резервное копирование информации. Создание RAID-массивов. Зеркалирование серверов.
31. Методы шифрования. Симметричное шифрование. Блочное шифрование. Поточное шифрование.
32. Блочные шифры. Шифры перестановок. Шифры замены.
33. Шифры замены. Моноалфавитные шифры. Шифр с подстановкой Цезаря.
34. Шифры замены. Полиалфавитные шифры. Шифр с подстановками Виженера.
35. Кодирование в автоключевой системе Виженера.
36. Система одноразового шифрования. Шифр Вернама.
37. Поточные шифры. Регистры сдвига с обратной связью.
38. Поточный шифр A5.
39. Методы продукционного шифрования. Сеть Фейстеля.
40. Стандарты шифрования данных DES и AES.
41. Односторонние функции. Ключевой обмен Диффи-Хеллмана.
42. Алгоритм RSA.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В КФУ действует балльно-рейтинговая система оценки знаний обучающихся. Суммарно по дисциплине (модулю) можно получить максимум 100 баллов за семестр, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов.

Для зачёта:

56 баллов и более - "зачтено".

55 баллов и менее - "не зачтено".

Для экзамена:

86 баллов и более - "отлично".

71-85 баллов - "хорошо".

56-70 баллов - "удовлетворительно".

55 баллов и менее - "неудовлетворительно".

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
Семестр 1			
Текущий контроль			
Тестирование	Тестирование проходит в письменной форме или с использованием компьютерных средств. Обучающийся получает определённое количество тестовых заданий. На выполнение выделяется фиксированное время в зависимости от количества заданий. Оценка выставляется в зависимости от процента правильно выполненных заданий.	1	6
Лабораторные работы	В аудитории, оснащённой соответствующим оборудованием, обучающиеся проводят учебные эксперименты и тренируются в применении практико-ориентированных технологий. Оцениваются знание материала и умение применять его на практике, умения и навыки по работе с оборудованием в соответствующей предметной области.	2	12
Семестр 2			
Текущий контроль			
Тестирование	Тестирование проходит в письменной форме или с использованием компьютерных средств. Обучающийся получает определённое количество тестовых заданий. На выполнение выделяется фиксированное время в зависимости от количества заданий. Оценка выставляется в зависимости от процента правильно выполненных заданий.	1	6
Лабораторные работы	В аудитории, оснащённой соответствующим оборудованием, обучающиеся проводят учебные эксперименты и тренируются в применении практико-ориентированных технологий. Оцениваются знание материала и умение применять его на практике, умения и навыки по работе с оборудованием в соответствующей предметной области.	2	18
Реферат	Обучающиеся самостоятельно пишут работу на заданную тему и сдают преподавателю в письменном виде. В работе производится обзор материала в определённой тематической области либо предлагается собственное решение определённой теоретической или практической проблемы. Оцениваются проработка источников, изложение материала, формулировка выводов, соблюдение требований к структуре и оформлению работы, своевременность выполнения. В случае публичной защиты реферата оцениваются также ораторские способности.	3	8
Зачет	Зачёт нацелен на комплексную проверку освоения дисциплины. Обучающийся получает вопрос (вопросы) либо задание (задания) и время на подготовку. Зачёт проводится в устной, письменной или компьютерной форме. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.		50

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература:

1. Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: ИЦ РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Режим доступа: http://znanium.com/go.php?id=405000.

2. Баранова Е.К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. - 4-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2019. - 322 с. - (Высшее образование). - ww.dx.doi.org/10.12737/11380. - ISBN : 978-5-369-01761-6.- Режим доступа: http://znanium.com/catalog/product/1009606

3. Тимошкин А. И. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - М.: РИОР: ИНФРА-М, 2019. - 400 с.ISBN: 978-5-369-01759-3 - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3 - Режим доступа: http://znanium.com/catalog/product/1018901

7.2. Дополнительная литература:

1. Хорев П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учебное пособие для вузов / П. Б. Хорев .- 3-е изд., стер .- Москва : Академия, 2007 .? 256 с. : ил., табл.- (Высшее профессиональное образование) .- Рек. УМО .- В пер .- Библиогр.: с. 251-252 .- ISBN 978-5-7695-4157-5 (10 экз.)

2.Куприянов А. И. Основы защиты информации [Текст] : учебное пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов .- 2-е изд., стер .- Москва : Академия, 2007 .- 256 с. : ил., табл. - (Высшее профессиональное образование) (Радиоэлектроника) .- Гриф УМО .- В пер .- Библиогр.: с. 251-252 .- ISBN 978-5-7695-4416-3 : 276-38 : 196-68 : 197-37 : 189-30 : 216-60 (29 экз.)

3. Мельников В. П. Информационная безопасность [Текст] : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова .- 8-е изд., испр .- Москва : Академия, 2013 .- 336 с : ил .- (Среднее профессиональное образование) .- Гриф МО .- В пер .- Библиогр.: с. 327-328. (10 экз.)

4. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] : учебное пособие для вузов / А. А. Малюк .- Москва : Горячая линия-Телеком, 2004 .-280с : ил., табл .-Прил.: с. 233-275 .-Гриф МО .- Библиогр.: с.276-278 .- ISBN 5-93517-197-X : 98-34. (26 экз.)

5. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. - М. : ИД 'ФОРУМ' : ИНФРА-М, 2019. - 592 с.-

ISBN: 978-5-8199-0730-6 - (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/996789

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Computers & Applied Sciences Complete - http://search.ebscohost.com/

ЭБС "Знание" - http://znanium.com/

ЭБС "Лань" - http://e.lanbook.com/

ЭБС "Научная электронная библиотека" - http://eLIBRARY.RU

Электронная библиотека "Academic Complete" - http://site.ebrary.com/lib/kazanst/

Энциклопедия "Википедия" - http://ru.wikipedia.org

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	В ходе лекционных занятий вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. В ходе подготовки к семинарам изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д. При этом учесть рекомендации преподавателя и требования учебной программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой. Подготовить тезисы для выступлений по всем учебным вопросам, выносимым на семинар. Готовясь к докладу или реферативному сообщению, обращаться за методической помощью к преподавателю. Составить план-конспект своего выступления. Продумать примеры с целью обеспечения тесной связи изучаемой теории с реальной жизнью. Своевременное и качественное выполнение самостоятельной работы базируется на соблюдении настоящих рекомендаций и изучении рекомендованной литературы. Студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании курсовых и дипломных работ.

Вид работ	Методические рекомендации
практические занятия	В процессе практического занятия как вида учебных занятий студенты выполняют одну или несколько практических работ (заданий) под руководством преподавателя в соответствии с изучаемым содержанием учебного материала. Выполнение студентами практических занятий направлено на: - обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины; - формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности; - развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.; - выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.
лабораторные работы	Работа на лабораторных занятиях предполагает активную проработку поставленных вопросов и задач с использованием известных методик настройки подсистем, способов программирования и подключения соответствующих библиотек. Для подготовки к занятиям рекомендуется обращать внимание на проблемные вопросы, затрагиваемые преподавателем в лекции, и группировать информацию вокруг них. Желательно выделять в используемой литературе постановки вопросов, на которые разными авторам могут быть даны различные ответы. На основании постановки таких вопросов следует собирать аргументы в пользу различных вариантов решения поставленных проблем. В текстах авторов, таким образом, следует выделять следующие компоненты: - постановка проблемы; - варианты решения; - аргументы в пользу тех или иных вариантов решения. На основе выделения этих элементов проще составлять собственную аргументированную позицию по рассматриваемому вопросу. В тестовых заданиях в каждом вопросе из представленных вариантов ответа правильный только один. Если Вам кажется, что правильных ответов больше, выбирайте тот, который, на Ваш взгляд, наиболее правильный. При подготовке к экзамену необходимо опираться прежде всего на лекции, а также на источники, которые разбирались на семинарах и практических занятиях в течение семестра. В каждом билете на экзамен содержатся 5 вопросов и тематическая задача.

Вид работ	Методические рекомендации
самостоя-тельная работа	Методические указания направлены на оказание методической помощи обучающимся при выполнении внеаудиторных самостоятельных работ. Выполнение внеаудиторных самостоятельных работ обучающимися в процессе изучения курса является важнейшим этапом обучения, который способствует систематизации и закреплению полученных теоретических знаний и практических умений; формированию навыков работы с различными видами информации, развитию познавательных способностей и активности обучающихся, формированию таких качеств личности, как ответственность и организованность, самостоятельность мышления, способность к саморазвитию, самосовершенствованию и самореализации, воспитывать самостоятельность как личностное качество будущего рабочего. В настоящее время актуальным становятся требования к личным качествам современного обучающегося ? умению самостоятельно пополнять и обновлять знания, вести самостоятельный поиск необходимого материала, быть творческой личностью. Внеаудиторная самостоятельная работа обучающихся, является обязательной для каждого обучающегося, определяется учебным планом. Её необходимо организовывать так, чтобы обучающийся постоянно преодолевал посильные трудности, но чтобы уровень требований, предъявляемых к обучающемуся, не был ниже уровня развития его умственных способностей. Цель методических указаний состоит в обеспечении эффективности самостоятельной работы, определении ее содержания, установления требований к оформлению и результатам самостоятельной работы. Основными целями внеаудиторной самостоятельной работы обучающихся являются: - овладение знаниями, профессиональными умениями и навыками деятельности по профилю специальности; приобретение способности к самостоятельному поиску работы и трудоустройства; - формирование готовности к самообразованию, самостоятельности и ответственности; - развитие творческого подхода к решению проблем учебного и профессионального уровня. Выполнение обучающимися внеаудиторных самостоятельных работ способствует формированию профессиональных и общих компетенций, соответствующих виду профессиональной деятельности по дисциплинам и профессиональным модулям. Самостоятельные работы выполняются индивидуально в свободное от занятий время. Обучающийся обязан: - перед выполнением самостоятельной работы, повторить теоретический материал, пройденный на аудиторных занятиях; - выполнить работу согласно заданию; - по каждой самостоятельной работе представить преподавателю отчет в письменном виде. - ответить на поставленные вопросы.
тестирование	При самостоятельной подготовке к тестированию студенту необходимо: а) готовясь к тестированию, проработайте информационный материал по дисциплине. Проконсультируйтесь с преподавателем по вопросу выбора учебной литературы; б) четко выясните все условия тестирования заранее. Вы должны знать, сколько тестов Вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д. в) приступая к работе с тестами, внимательно и до конца прочтите вопрос и предлагаемые варианты ответов. Выберите правильные (их может быть несколько). На отдельном листке ответов выпишите цифру вопроса и буквы, соответствующие правильным ответам; г) в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант. д) если Вы встретили чрезвычайно трудный для Вас вопрос, не тратьте много времени на него. Переходите к другим тестам. Вернитесь к трудному вопросу в конце. е) обязательно оставьте время для проверки ответов, чтобы избежать механических ошибок.

Вид работ	Методические рекомендации
реферат	Требования к оформлению реферата Объем реферата 20 - 25 стр. печатного текста. Шрифт - не более 14 pt, TimesNewRoman, интервал - 1,5, поля: верхнее, нижнее, левое 2 см, правое 1,5 см. На титульном листе указывается название работы, ФИО студента и группа, ФИО преподавателя (научного руководителя), проверяющего и оценивающего реферат, наименование кафедры и учебного заведения. Тема реферата может быть сформулирована самостоятельно, по согласованию с преподавателем. Название работы оформляется следующим образом: Реферат по дисциплине ?Операционные системы? на тему: ???? Текст реферата печатается на одной стороне страницы; сноски и примечания печа-таются на той же странице, к которой они относятся (через 1 интервал, более мелким шрифтом, чем текст). Основной текст должен сопровождаться иллюстративным материалом (рисунки, фотографии, диаграммы, схемы, таблицы, программы). Если в основной части содержатся цитаты или ссылки на высказывания, необходимо указать номер источника по списку, приведенному в конце реферата, и страницу в квадратных скобках в конце цитаты или ссылки. Реферат ? это краткое изложение в письменной форме содержания прочитанных книг и документов; сообщение об итогах изучения научного вопроса; доклад на определенную тему, освещающий ее вопросы на основе литературных и других источников. Целью написания реферата является углубление знаний по конкретной проблеме, получение навыков работы с научной и научно-популярной литературой. Работа над рефератом требует, как правило, не менее месяца. В процессе работы над проблемой необходимо: ? вычленить проблему; ? самостоятельно изучить проблему на основе первоисточников; ? дать обзор использованной литературы; ? последовательно и доказательно изложить материал; ? правильно оформить ссылки на источники. 2. Обязательные структурные элементы реферата: 1. Введение, в котором описывается актуальность проблемы, определяются цели и задача реферата; объем введения ? 1 - 2 страницы. 2. Содержание. 3. Текст реферата должен содержать: ? обоснование выбранной темы; ? сравнительный анализ литературы по проблеме; ? изложение собственной точки зрения на проблему; ? выводы и предложения; ? заключение. 4. Список использованных источников должен оформляться в соответствии с ГОСТом и может содержать не только названия книг, журналов, газет, но и любые источники информации (например, сведения из сети Интернет, информацию из теле- и радио-передач, а также частные сообщения каких-либо специалистов, высказанные в личных беседах их с автором реферата). Реферат излагается доступным научным (научно-популярным) языком в относи-тельно сжатой форме с использованием облегченных синтаксических конструкций. Такие конструкции могут стать своеобразным планом реферативной статьи: ? В рассматриваемой статье ставится ряд вопросов ?Автор подчеркивает, что ? Более подробно рассмотрена проблема? Анализируются разные точки зрения ? В заключение необходимо от-метить что ?? и т.д. При выставлении оценки за реферат учитываются следующие компоненты: ? содержательная часть (глубина проработки проблемы, структура работы, объем проанализированных источников и т.п.); ? оформление (соответствие стандарту, эстетика оформления, наличие иллюстративного материала и т.п.); ? защита реферата (ориентация в тексте реферата, ответы на вопросы и т.п.). Реферат сдается в отпечатанном виде и на электронном носителе.

Вид работ	Методические рекомендации
зачет	Готовиться к зачету необходимо последовательно, с учетом контрольных вопросов, разработанных ведущим преподавателем кафедры. Сначала следует определить место каждого контрольного вопроса в соответствующем разделе темы учебной программы, а затем внимательно прочитать и осмыслить рекомендованные научные работы, соответствующие разделы рекомендованных учебников. При этом полезно делать хотя бы самые краткие выписки и заметки. Работу над темой можно считать завершенной, если вы сможете ответить на все контрольные вопросы и дать определение понятий по изучаемой теме. Для обеспечения полноты ответа на контрольные вопросы и лучшего запоминания теоретического материала рекомендуется составлять план ответа на контрольный вопрос. Это позволит сэкономить время для подготовки непосредственно перед зачетом за счет обращения не к литературе, а к своим записям. При подготовке необходимо выявлять наиболее сложные, дискуссионные вопросы, с тем, чтобы обсудить их с преподавателем на обзорных лекциях и консультациях. Нельзя ограничивать подготовку к зачету простым повторением изученного материала. Необходимо углубить и расширить ранее приобретенные знания за счет новых идей и положений. Результат по сдаче зачета объявляется студентам, вносится в экзаменационную ведомость. Незачет проставляется только в ведомости. После чего студент освобождается от дальнейшего присутствия на зачете. При получении незачета повторная сдача осуществляется в другие дни, установленные деканатом. Положительная оценка 'зачтено' выставляется, если студент усвоил учебный материал, исчерпывающе, логически, грамотно изложив его, показал знания специальной литературы, не допускал существенных неточностей, а также правильно применял понятийный аппарат.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Освоение дисциплины "Безопасность информационных систем" предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows Professional 7 Russian

Пакет офисного программного обеспечения Microsoft Office 2010 Professional Plus Russian

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. 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, учебно-методические комплексы, 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 образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. 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.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Освоение дисциплины "Безопасность информационных систем" 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.

Специализированная лаборатория оснащена оборудованием, необходимым для проведения лабораторных работ, практических занятий и самостоятельной работы по отдельным дисциплинам, а также практик и научно-исследовательской работы обучающихся. Лаборатория рассчитана на одновременную работу обучающихся академической группы либо подгруппы. Занятия проводятся под руководством сотрудника университета, контролирующего выполнение видов учебной работы и соблюдение правил техники безопасности. Качественный и количественный состав оборудования и расходных материалов определяется спецификой образовательных программ.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 09.04.01 "Информатика и вычислительная техника" и магистерской программе Автоматизированные системы обработки информации и управления .