МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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.

Программа дисциплины

Защита информации Б1.В.ОД.16

Направление подготовки: 09.03.04 - Программная инженерия
Профиль подготовки: Разработка программно-информационных систем
Квалификация выпускника: бакалавр
Форма обучения: заочное
Язык обучения: русский
Год начала обучения по образовательной программе: 2016
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.

Набережные челны
2018

Содержание

Программу дисциплины разработал(а)(и) старший преподаватель, 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-4	владением концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества

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.

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

Данная учебная дисциплина включена в раздел "Б1.В.ОД.16 Дисциплины (модули)" основной профессиональной образовательной программы 09.03.04 "Программная инженерия (Разработка программно-информационных систем)" и относится к обязательным дисциплинам.
Осваивается на 5 курсе в 9, 10 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 - 22 часа(ов), в том числе лекции - 8 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 14 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 113 часа(ов).

Контроль (зачёт / экзамен) - 9 часа(ов).

Форма промежуточного контроля дисциплины: отсутствует в 9 семестре; экзамен в 10 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	Раздел 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	9	0	0	1	
2.	Тема 2. Основы информационной безопасности	9	1	0	1	
3.	Тема 3. Безопасность операционных систем	9	1	0	1	
4.	Тема 4. Безопасность вычислительных сетей	9	1	0	1	
5.	Тема 5. Безопасность систем управления базами данных	9	1	0	2	
6.	Тема 6. Организационное обеспечение информационной безопасности	10	1	0	2	17
7.	Тема 7. Программно-аппаратные средства защиты информации	10	1	0	2	32
8.	Тема 8. Криптографические методы защиты информации	10	1	0	2	32
9.	Тема 9. Комплексное обеспечение информационной безопасности автоматизированных систем	10	1	0	2	32
	Итого		8	0	14	113

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.

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.

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.

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.

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.

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.

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.

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.

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.

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 N301).

Письмо Министерства образования Российской Федерации N14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Положение от 24 декабря 2015 г. № 0.1.1.67-06/265/15 "О порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет""

Положение N 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 N 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 N 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 N 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 N 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 9			
	Текущий контроль		
1	Тестирование	ПК-4	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-4	1. Правовое обеспечение информационной безопасности 2. Основы информационной безопасности 3. Безопасность операционных систем 4. Безопасность вычислительных сетей 5. Безопасность систем управления базами данных

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
Семестр 10			
	Текущий контроль		
1	Тестирование	ПК-4	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-4	6. Организационное обеспечение информационной безопасности 7. Программно-аппаратные средства защиты информации 8. Криптографические методы защиты информации 9. Комплексное обеспечение информационной безопасности автоматизированных систем
	Экзамен	ПК-4	

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 9					
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 10					
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

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Экзамен	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании, изложении и использовании учебно-программного материала.	Обучающийся обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные программой задания, усвоил основную литературу, рекомендованную программой дисциплины, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой дисциплины, допустил погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	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 9

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

2. Лабораторные работы

Темы 1, 2, 3, 4, 5
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.

Обеспечение безопасности электронной почты при работе в сети Интернет.
Отработка безопасных механизмов работы с почтой в сети Интернет.

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

Использование межсетевых экранов при работе в локальной вычислительной сети предприятия и сети Интернет.
Изучение принципов работы и возможностей программных средств обеспечения сетевой безопасности.

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.

Семестр 10
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.

2. Лабораторные работы

Темы 6, 7, 8, 9

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.

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.

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.

Методы выявления каналов НСД.

Экзамен

Вопросы к экзамену:

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 9			
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	12
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	13
Семестр 10			
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	12
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	13
		Всего:	50
Экзамен	Экзамен нацелен на комплексную проверку освоения дисциплины. Экзамен проводится в устной или письменной форме по билетам, в которых содержатся вопросы (задания) по всем темам курса. Обучающемуся даётся время на подготовку. 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. Васильев В. И. Интеллектуальные системы защиты информации [Электронный ресурс] : учебное пособие / В. И. Васильев. - Москва: Машиностроение, 2013. - 171 с. - ISBN 978-5-94275-667-3. - Режим доступа: http://e.lanbook.com/view/book/5792.

3. Кузнецов И. Н. Бизнес-безопасность [Электронный ресурс] / И. Н. Кузнецов. - Москва: Издательско-торговая корпорация 'Дашков и К', 2013. - 416 с. - ISBN 978-5-394-01438-3. ;http://znanium.com/go.php?id=430343.

4.Применение искусственных нейронных сетей и системы остаточных классов в криптографии [Электронный ресурс] / [Н. И. Червяков и др.]. - Москва: Физматлит, 2012. - 279 с. - ISBN 978-5-9221-1386-1. - :http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5300.

5.Шаньгин В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]: учебное пособие / В. Ф. Шаньгин. - Москва: ФОРУМ, 2013. - 592 с. - ISBN 978-5-8199-0411-4. - Режим доступа: http://znanium.com/go.php?id=402686.

7.2. Дополнительная литература:

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для студ. вузов по напр. 230100 (654600) / П. Б. Хорев. - 3-е изд., стер. - М.: Академия, 2007. - 256 с.

2. Куприянов А.И. Основы защиты информации: учебное пособие для студентов высш. учеб. заведений. - М.: Издательский центр 'Академия', 2007. - 256с.

3. Мельников В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 4-е изд., стер. - Москва : Академия, 2009. - 336 с. : ил., табл. - (Высшее профессиональное образование). - Библиогр.: с. 327-328. - Рек. УМО. - В пер. - ISBN 978-5-7695-6150-4.

4. 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). - Библиогр.: с. 327-328. - Гриф МО. - В пер. - ISBN 978-5-7695-9954-5

5. Емельянова Н. З., Партыка Т. Л., Попов И. И. Защита информации в персональном компьютере: учебное пособие. - М.: ФОРУМ, 2009. - 368с.

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

Консультант студента. Электронная библиотека - studentlibrary.ru

ЭБС ?Знание? - http://znanium.com

ЭБС ?Лань? - http://e.lanbook.com

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

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.

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

Освоение дисциплины "Защита информации" 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 Google Chrome

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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.

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

Освоение дисциплины "Защита информации" 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.

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 09.03.04 "Программная инженерия" и профилю подготовки Разработка программно-информационных систем .