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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.

подписано электронно-цифровой подписью

Программа дисциплины

Введение в криптографию Б2.ДВ.1

Направление подготовки: 010400.62 - Прикладная математика и информатика
Профиль подготовки: Математическая кибернетика
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Кугураков В.С.

Рецензент(ы):

СОГЛАСОВАНО:

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

Регистрационный No 99114

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Кугураков В.С. кафедра теоретической кибернетики отделение фундаментальной информатики и информационных технологий , Vladimir.Kugurakov@kpfu.ru

1. Цели освоения дисциплины

Дисциплина знакомит студентов с криптографическими методами защиты информации от несанкционированного доступа. Основная цель дисциплины - научить пониманию необходимости обеспечения комплексной безопасности информационных систем, получить практические знания и навыки для простейшей организации криптографически защищенной системы.

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

Данная учебная дисциплина включена в раздел " Б2.ДВ.1 Общепрофессиональный" основной образовательной программы 010400.62 Прикладная математика и информатика и относится к дисциплинам по выбору. Осваивается на 2 курсе, 4 семестр.

Данная дисциплина относится к общепрофессиональным дисциплинам.

Читается на 2 курсе 4 семестр для студентов, обучающихся по направлению "Прикладная математика и информатика".

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-11 (профессиональные компетенции)	способность приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности

В результате освоения дисциплины студент:

1. должен знать:

необходимости обеспечения комплексной информационной безопасности любых объектов;

2. должен уметь:

ориентироваться в существующих системах криптографической защиты информации;

3. должен владеть:

теоретическими знаниями о методах криптографической защиты информации;

4. должен демонстрировать способность и готовность:

приобрести навыки простейшей организации защиты информационных систем.

4. Структура и содержание дисциплины/ модуля

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

Форма промежуточного контроля дисциплины экзамен в 4 семестре.

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

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);
55-70 баллов - "удовлетворительно" (удов.);
54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение. Цель и задачи курса. Структура курса и его связь с другими дисциплинами. Краткий исторический очерк о развитии систем защиты информации в России и за рубежом. Информационная безопасность компьютерных систем. Основные понятия и определения. Основные угрозы безопасности автоматизированных систем обработки информации (АСОИ). Обеспечение безопасности АСОИ. Принципы криптографической защиты информации. Основные приложения современной криптографии. Аппаратные и программные средства защиты информации	4		2	0	4	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Формальные модели криптосистем. Надежность шифров. Теоретическая и практическая стойкость шифров. Классификация шифров по различным признакам. Классические симметричные криптосистемы. Шифры-перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифрование методом гаммирования. Абсолютно стойкий шифр.	4		2	0	4	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Современные симметричные криптосистемы (блочные системы шифрования). Принципы построения блочных шифров. Принцип итерирования. Схема Фейстеля. Стандарты блочного шифрования. Федеральный стандарт США DES. Российский стандарт шифрования данных ГОСТ-28147-89. Известные блочные шифры: IDEA, RC-5, BlowFish, CAST-128 и т.п.. Новые стандарты криптографической защиты информации: шифр Rijndael и др. Режимы использования блочных шифров: ECB, CBC, CFB, OFB. Режимы шифрования данных российского стандарта. Комбинирование алгоритмов блочного шифрования. Криптосистемы с депонированием ключей. Криптоалгоритм Skipjack. Стандарт криптографической защиты AES. Атаки на блочные шифры.	4		2	0	4	
4.	Тема 4. Поточные шифры. Принципы построения поточных шифров. Примеры поточных криптосистем (RC4, A5, Panama, SNOW и др.). Генераторы псевдослучайных последовательностей.	4		2	0	4	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
5.	Тема 5. Асимметрические криптосистемы (системы шифрования с открытым ключом). Принципы построения асимметрических криптосистем. Теоретико-числовой и алгебраический аппарат, используемый при построении асимметрических криптосистем. Криптоалгоритмы RSA и Эль-Гамаля; криптография на основе эллиптических кривых над конечными полями.	4		2	0	4	
6.	Тема 6. Идентификация и проверка подлинности. Основные понятия и концепции. Идентификация и аутентификация. Особенности применения паролей для идентификации пользователя. Взаимная проверка пользователей. Протоколы идентификации. Аутентификация сообщений и функции хэширования. Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функций ГОСТ Р.34.11-94.	4		2	0	4	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
7.	Тема 7. Цифровая подпись. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы создания электронной цифровой подписи (RSA, EGSA, ECDSA). Стандарты цифровой подписи. Алгоритм цифровой подписи DSA. Российский стандарт цифровой подписи ГОСТ Р.34.10-94. Цифровые подписи с дополнительными функциональными возможностями: схема слепой цифровой подписи, схема неоспоримой подписи.	4		2	0	4	
8.	Тема 8. Управление криптографическими ключами. Генерация ключей. Хранение ключей. Концепция ключевого пространства и иерархия ключей. Распределение ключей. Протоколы распределения ключей. Передача ключей с использование симметричного шифрования. Двусторонние и трехсторонние протоколы. Передача ключей с использованием асимметричных систем шифрования. Протоколы без использования и с использованием цифровой подписи. Протокол Kerberos.	4		2	0	4	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
9.	Тема 9. Практические аспекты применения криптосистем. Требования к криптосистемам. Длина ключа и стойкость. Шифрование и архивирование. Шифрование и кодирование. Стандартизация алгоритмов шифрования.	4		2	0	4	
.	Тема . Итоговая форма контроля	4		0	0	0	экзамен
	Итого			18	0	36	

4.2 Содержание дисциплины

Тема 1. Введение. Цель и задачи курса. Структура курса и его связь с другими дисциплинами. Краткий исторический очерк о развитии систем защиты информации в России и за рубежом. Информационная безопасность компьютерных систем. Основные понятия и определения. Основные угрозы безопасности автоматизированных систем обработки информации (АСОИ). Обеспечение безопасности АСОИ. Принципы криптографической защиты информации. Основные приложения современной криптографии. Аппаратные и программные средства защиты информации

лекционное занятие (2 часа(ов)):

Введение. Цель и задачи курса. Структура курса и его связь с другими дисциплинами. Краткий исторический очерк о развитии систем защиты информации в России и за рубежом. Информационная безопасность компьютерных систем. Основные понятия и определения. Основные угрозы безопасности автоматизированных систем обработки информации (АСОИ). Обеспечение безопасности АСОИ. Принципы криптографической защиты информации. Основные приложения современной криптографии. Аппаратные и программные средства защиты информации

лабораторная работа (4 часа(ов)):

Тема 2. Формальные модели криптосистем. Надежность шифров. Теоретическая и практическая стойкость шифров. Классификация шифров по различным признакам. Классические симметричные криптосистемы. Шифры-перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифрование методом гаммирования. Абсолютно стойкий шифр.

лекционное занятие (2 часа(ов)):

Формальные модели криптосистем. Надежность шифров. Теоретическая и практическая стойкость шифров. Классификация шифров по различным признакам. Классические симметричные криптосистемы. Шифры-перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифрование методом гаммирования. Абсолютно стойкий шифр.

лабораторная работа (4 часа(ов)):

Тема 3. Современные симметричные криптосистемы (блочные системы шифрования). Принципы построения блочных шифров. Принцип итерирования. Схема Фейстеля. Стандарты блочного шифрования. Федеральный стандарт США DES. Российский стандарт шифрования данных ГОСТ-28147-89. Известные блочные шифры: IDEA, RC-5, BlowFish, CAST-128 и т.п.. Новые стандарты криптографической защиты информации: шифр Rijndael и др. Режимы использования блочных шифров: ECB, CBC, CFB, OFB. Режимы шифрования данных российского стандарта. Комбинирование алгоритмов блочного шифрования. Криптосистемы с депонированием ключей. Криптоалгоритм Skipjack. Стандарт криптографической защиты AES. Атаки на блочные шифры.

лекционное занятие (2 часа(ов)):

Современные симметричные криптосистемы (блочные системы шифрования). Принципы построения блочных шифров. Принцип итерирования. Схема Фейстеля. Стандарты блочного шифрования. Федеральный стандарт США DES. Российский стандарт шифрования данных ГОСТ-28147-89. Известные блочные шифры: IDEA, RC-5, BlowFish, CAST-128 и т.п.. Новые стандарты криптографической защиты информации: шифр Rijndael и др. Режимы использования блочных шифров: ECB, CBC, CFB, OFB. Режимы шифрования данных российского стандарта. Комбинирование алгоритмов блочного шифрования. Криптосистемы с депонированием ключей. Криптоалгоритм Skipjack. Стандарт криптографической защиты AES. Атаки на блочные шифры.

лабораторная работа (4 часа(ов)):

Тема 4. Поточные шифры. Принципы построения поточных шифров. Примеры поточных криптосистем (RC4, A5, Panama, SNOW и др.). Генераторы псевдослучайных последовательностей.

лекционное занятие (2 часа(ов)):

Поточные шифры. Принципы построения поточных шифров. Примеры поточных криптосистем (RC4, A5, Panama, SNOW и др.). Генераторы псевдослучайных последовательностей.

лабораторная работа (4 часа(ов)):

Тема 5. Асимметрические криптосистемы (системы шифрования с открытым ключом). Принципы построения асимметрических криптосистем. Теоретико-числовой и алгебраический аппарат, используемый при построении асимметрических криптосистем. Криптоалгоритмы RSA и Эль-Гамаля; криптография на основе эллиптических кривых над конечными полями.

лекционное занятие (2 часа(ов)):

Асимметрические криптосистемы (системы шифрования с открытым ключом). Принципы построения асимметрических криптосистем. Теоретико-числовой и алгебраический аппарат, используемый при построении асимметрических криптосистем. Криптоалгоритмы RSA и Эль-Гамаля; криптография на основе эллиптических кривых над конечными полями

лабораторная работа (4 часа(ов)):

Тема 6. Идентификация и проверка подлинности. Основные понятия и концепции. Идентификация и аутентификация. Особенности применения паролей для идентификации пользователя. Взаимная проверка пользователей. Протоколы идентификации. Аутентификация сообщений и функции хэширования. Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функций ГОСТ Р.34.11-94.

лекционное занятие (2 часа(ов)):

Идентификация и проверка подлинности. Основные понятия и концепции. Идентификация и аутентификация. Особенности применения паролей для идентификации пользователя. Взаимная проверка пользователей. Протоколы идентификации. Аутентификация сообщений и функции хэширования. Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функций ГОСТ Р.34.11-94.

лабораторная работа (4 часа(ов)):

Тема 7. Цифровая подпись. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы создания электронной цифровой подписи (RSA, EGSA, ECDSA). Стандарты цифровой подписи. Алгоритм цифровой подписи DSA. Российский стандарт цифровой подписи ГОСТ Р.34.10-94. Цифровые подписи с дополнительными функциональными возможностями: схема слепой цифровой подписи, схема неоспоримой подписи.

лекционное занятие (2 часа(ов)):

Цифровая подпись. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы создания электронной цифровой подписи (RSA, EGSA, ECDSA). Стандарты цифровой подписи. Алгоритм цифровой подписи DSA. Российский стандарт цифровой подписи ГОСТ Р.34.10-94. Цифровые подписи с дополнительными функциональными возможностями: схема слепой цифровой подписи, схема неоспоримой подписи.

лабораторная работа (4 часа(ов)):

Тема 8. Управление криптографическими ключами. Генерация ключей. Хранение ключей. Концепция ключевого пространства и иерархия ключей. Распределение ключей. Протоколы распределения ключей. Передача ключей с использование симметричного шифрования. Двусторонние и трехсторонние протоколы. Передача ключей с использованием асимметричных систем шифрования. Протоколы без использования и с использованием цифровой подписи. Протокол Kerberos.

лекционное занятие (2 часа(ов)):

Управление криптографическими ключами. Генерация ключей. Хранение ключей. Концепция ключевого пространства и иерархия ключей. Распределение ключей. Протоколы распределения ключей. Передача ключей с использование симметричного шифрования. Двусторонние и трехсторонние протоколы. Передача ключей с использованием асимметричных систем шифрования. Протоколы без использования и с использованием цифровой подписи. Протокол Kerberos.

лабораторная работа (4 часа(ов)):

Тема 9. Практические аспекты применения криптосистем. Требования к криптосистемам. Длина ключа и стойкость. Шифрование и архивирование. Шифрование и кодирование. Стандартизация алгоритмов шифрования.

лекционное занятие (2 часа(ов)):

Практические аспекты применения криптосистем. Требования к криптосистемам. Длина ключа и стойкость. Шифрование и архивирование. Шифрование и кодирование. Стандартизация алгоритмов шифрования.

лабораторная работа (4 часа(ов)):

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Введение. Цель и задачи курса. Структура курса и его связь с другими дисциплинами. Краткий исторический очерк о развитии систем защиты информации в России и за рубежом. Информационная безопасность компьютерных систем. Основные понятия и определения. Основные угрозы безопасности автоматизированных систем обработки информации (АСОИ). Обеспечение безопасности АСОИ. Принципы криптографической защиты информации. Основные приложения современной криптографии. Аппаратные и программные средства защиты информации	4		подготовка домашнего задания	6	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Формальные модели криптосистем. Надежность шифров. Теоретическая и практическая стойкость шифров. Классификация шифров по различным признакам. Классические симметричные криптосистемы. Шифры-перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифрование методом гаммирования. Абсолютно стойкий шифр.	4		подготовка домашнего задания	6	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
3.	Тема 3. Современные симметричные криптосистемы (блочные системы шифрования). Принципы построения блочных шифров. Принцип итерирования. Схема Фейстеля. Стандарты блочного шифрования. Федеральный стандарт США DES. Российский стандарт шифрования данных ГОСТ-28147-89. Известные блочные шифры: IDEA, RC-5, BlowFish, CAST-128 и т.п.. Новые стандарты криптографической защиты информации: шифр Rijndael и др. Режимы использования блочных шифров: ECB, CBC, CFB, OFB. Режимы шифрования данных российского стандарта. Комбинирование алгоритмов блочного шифрования. Криптосистемы с депонированием ключей. Криптоалгоритм Skipjack. Стандарт криптографической защиты AES. Атаки на блочные шифры.	4		подготовка домашнего задания	6	домашнее задание
4.	Тема 4. Поточные шифры. Принципы построения поточных шифров. Примеры поточных криптосистем (RC4, A5, Panama, SNOW и др.). Генераторы псевдослучайных последовательностей.	4		подготовка домашнего задания	6	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
5.	Тема 5. Асимметрические криптосистемы (системы шифрования с открытым ключом). Принципы построения асимметрических криптосистем. Теоретико-числовой и алгебраический аппарат, используемый при построении асимметрических криптосистем. Криптоалгоритмы RSA и Эль-Гамаля; криптография на основе эллиптических кривых над конечными полями.	4		подготовка домашнего задания	6	домашнее задание
6.	Тема 6. Идентификация и проверка подлинности. Основные понятия и концепции. Идентификация и аутентификация. Особенности применения паролей для идентификации пользователя. Взаимная проверка пользователей. Протоколы идентификации. Аутентификация сообщений и функции хэширования. Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функций ГОСТ Р.34.11-94.	4		подготовка домашнего задания	6	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
7.	Тема 7. Цифровая подпись. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы создания электронной цифровой подписи (RSA, EGSA, ECDSA). Стандарты цифровой подписи. Алгоритм цифровой подписи DSA. Российский стандарт цифровой подписи ГОСТ Р.34.10-94. Цифровые подписи с дополнительными функциональными возможностями: схема слепой цифровой подписи, схема неоспоримой подписи.	4		подготовка домашнего задания	6	домашнее задание
8.	Тема 8. Управление криптографическими ключами. Генерация ключей. Хранение ключей. Концепция ключевого пространства и иерархия ключей. Распределение ключей. Протоколы распределения ключей. Передача ключей с использование симметричного шифрования. Двусторонние и трехсторонние протоколы. Передача ключей с использованием асимметричных систем шифрования. Протоколы без использования и с использованием цифровой подписи. Протокол Kerberos.	4		подготовка домашнего задания	6	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
9.	Тема 9. Практические аспекты применения криптосистем. Требования к криптосистемам. Длина ключа и стойкость. Шифрование и архивирование. Шифрование и кодирование. Стандартизация алгоритмов шифрования.	4		подготовка домашнего задания	6	домашнее задание
	Итого				54	

5. Образовательные технологии, включая интерактивные формы обучения

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

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

Тема 1. Введение. Цель и задачи курса. Структура курса и его связь с другими дисциплинами. Краткий исторический очерк о развитии систем защиты информации в России и за рубежом. Информационная безопасность компьютерных систем. Основные понятия и определения. Основные угрозы безопасности автоматизированных систем обработки информации (АСОИ). Обеспечение безопасности АСОИ. Принципы криптографической защиты информации. Основные приложения современной криптографии. Аппаратные и программные средства защиты информации

домашнее задание, примерные вопросы:

Тема 2. Формальные модели криптосистем. Надежность шифров. Теоретическая и практическая стойкость шифров. Классификация шифров по различным признакам. Классические симметричные криптосистемы. Шифры-перестановки. Блочные и поточные шифры простой замены. Многоалфавитные шифры замены. Шифрование методом гаммирования. Абсолютно стойкий шифр.

домашнее задание, примерные вопросы:

Тема 3. Современные симметричные криптосистемы (блочные системы шифрования). Принципы построения блочных шифров. Принцип итерирования. Схема Фейстеля. Стандарты блочного шифрования. Федеральный стандарт США DES. Российский стандарт шифрования данных ГОСТ-28147-89. Известные блочные шифры: IDEA, RC-5, BlowFish, CAST-128 и т.п.. Новые стандарты криптографической защиты информации: шифр Rijndael и др. Режимы использования блочных шифров: ECB, CBC, CFB, OFB. Режимы шифрования данных российского стандарта. Комбинирование алгоритмов блочного шифрования. Криптосистемы с депонированием ключей. Криптоалгоритм Skipjack. Стандарт криптографической защиты AES. Атаки на блочные шифры.

домашнее задание, примерные вопросы:

Тема 4. Поточные шифры. Принципы построения поточных шифров. Примеры поточных криптосистем (RC4, A5, Panama, SNOW и др.). Генераторы псевдослучайных последовательностей.

домашнее задание, примерные вопросы:

Тема 5. Асимметрические криптосистемы (системы шифрования с открытым ключом). Принципы построения асимметрических криптосистем. Теоретико-числовой и алгебраический аппарат, используемый при построении асимметрических криптосистем. Криптоалгоритмы RSA и Эль-Гамаля; криптография на основе эллиптических кривых над конечными полями.

домашнее задание, примерные вопросы:

Тема 6. Идентификация и проверка подлинности. Основные понятия и концепции. Идентификация и аутентификация. Особенности применения паролей для идентификации пользователя. Взаимная проверка пользователей. Протоколы идентификации. Аутентификация сообщений и функции хэширования. Функции хэширования и целостность данных. Ключевые и бесключевые функции хэширования. Примеры хэш-функций. Российский стандарт хэш-функций ГОСТ Р.34.11-94.

домашнее задание, примерные вопросы:

Тема 7. Цифровая подпись. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы создания электронной цифровой подписи (RSA, EGSA, ECDSA). Стандарты цифровой подписи. Алгоритм цифровой подписи DSA. Российский стандарт цифровой подписи ГОСТ Р.34.10-94. Цифровые подписи с дополнительными функциональными возможностями: схема слепой цифровой подписи, схема неоспоримой подписи.

домашнее задание, примерные вопросы:

Тема 8. Управление криптографическими ключами. Генерация ключей. Хранение ключей. Концепция ключевого пространства и иерархия ключей. Распределение ключей. Протоколы распределения ключей. Передача ключей с использование симметричного шифрования. Двусторонние и трехсторонние протоколы. Передача ключей с использованием асимметричных систем шифрования. Протоколы без использования и с использованием цифровой подписи. Протокол Kerberos.

домашнее задание, примерные вопросы:

Тема 9. Практические аспекты применения криптосистем. Требования к криптосистемам. Длина ключа и стойкость. Шифрование и архивирование. Шифрование и кодирование. Стандартизация алгоритмов шифрования.

домашнее задание, примерные вопросы:

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

По данной дисциплине предусмотрено проведение экзамена. Примерные вопросы для экзамена - Приложение1.

7.1. Основная литература:

1. Громкович, Ю. Теоретическая информатика: Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию. - Издание 3 - е. - СПб: БХВ - Петербург, 2010. - 336 с.

2. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с.

http://znanium.com/bookread.php?book=441493

3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с.

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

4. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - URL: http://kpfu.ru/docs/F366166681/mzi.pdf

7.2. Дополнительная литература:

1. Применко Э. А. Алгебраические основы криптографии: М.: URSS: [ЛИБРОКОМ, 2013]..283 с

2. Латыпов, Р. Х. Математические основы кодирования информации и криптографии: учеб. Пособие./ Казан. гос. ун - т. - Казань: [КГУ], 2005. - 59 с.

3. Земор, Жиль. Курс криптографии / Жиль Земор; пер. с фр. В.В. Шуликовской. - М.; Ижевск: Ин - т компьютер. исслед.: Регуляр. и хаотич. динамика, 2006. - 255 с

4. Введение в теоретико-числовые методы криптографии : учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090101 "Криптография" / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин .? Санкт-Петерург [и др.] : Лань, 2011 .? 394 с.

5. Молдовян, А.А. Криптография / А.А.Молдовян, Н.А.Молдовян, Б.Я.Советов .? СПб. : Лань, 2000 .? 218с. : табл., ил. ? (Учебники для вузов. Специальная литература) .? Авт. на обл. не указан .? Библиогр.: с.216-218 .? ISBN 5-8114-0246-5 : 53.10.

6. Введение в криптографию: Новые математические дисциплины : Учеб. / В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др.; Под ред. В.В.Ященко ; Под ред. В.В.Ященко .? СПб. и др. : Питер, 2001 .? 287с. ? Библиогр. в конце глав .? В кн. также: Теория связи в секретных системах/ К.Шеннона .? ISBN 5-318-00443-1 : 81.48.

7.3. Интернет-ресурсы:

Защита информации. Материалы - http://algolist.manual.ru/defence/intro.php

Криптографические стандарты - https://ru.wikipedia.org/wiki/%D1%F2%E0%ED%E4%E0%F0%F2%FB_%EA%F0%E8%EF%F2%EE%E3%

Криптография. Материалы - http://cryptography.ru/

Криптография. Определение, ссылки. Wikipedia - https://ru.wikipedia.org/wiki/%CA%F0%E8%EF%F2%EE%E3%F0%E0%F4%E8%FF

Курс по основам криптографии. ИНТУИТ - http://www.intuit.ru/studies/courses/691/547/info

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Введение в криптографию" предполагает использование следующего материально-технического обеспечения:

Лекционные занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером), а так же в специализированных компьютерных кабинетах.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010400.62 "Прикладная математика и информатика" и профилю подготовки Математическая кибернетика .

Автор(ы):
Кугураков В.С. _____
"__" _____ 201 __ г.

Рецензент(ы):
"__" _____ 201 __ г.