Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Криптографические методы защиты информации

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Курс: 3, семестр : 6

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**6**
1	Всего зачетных единиц (кредитов)	5
2	Всего часов	180
3	Всего занятий в контактной форме, час.	67
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	8
8	Аттестация, час.	2
9	Консультации, час.	11
10	Самостоятельная работа, час.	113
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	КР
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС введен в действие приказом №1509 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, базовая

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.ф-м.н. Котов Ю. А.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ПК.14** **способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации; *в части следующих результатов обучения*:**
у2. уметь проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации
***Компетенция ФГОС*: ПК.26 способность администрировать подсистему информационной безопасности автоматизированной системы; *в части следующих результатов обучения*:**
з2. знать место криптографических методов в подсистемах информационной безопасности объекта защиты
у1. уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	Формы организации занятий
Криптографические методы защиты информации	
ПК.14.у2 уметь проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации	
1.навыками использования ЭВМ в анализе простейших шифров	Лекции; Лабораторные работы; Самостоятельная работа
2.модели шифров и математические методы их исследования;	Лекции; Лабораторные работы; Самостоятельная работа
3.применять математические методы исследования моделей шифров;	Лекции; Лабораторные работы; Самостоятельная работа
4.криптографических и технических средств защиты информации;	Лекции; Лабораторные работы; Самостоятельная работа
5.проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;	Лекции; Лабораторные работы; Самостоятельная работа
ПК.26.з2 знать место криптографических методов в подсистемах информационной безопасности объекта защиты	
6.типовые шифры с открытыми ключами;	Лекции; Лабораторные работы; Самостоятельная работа
7.частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;	Лекции; Лабораторные работы; Самостоятельная работа
8.типовые поточные и блочные шифры;	Лекции; Лабораторные работы; Самостоятельная работа
9.требования к шифрам и основные характеристики шифров;	Лекции; Лабораторные работы; Самостоятельная работа
10.основные задачи и понятия криптографии;	Лекции; Лабораторные работы; Самостоятельная работа
ПК.26.у1 уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты	
11.навыками использования типовых криптографических алгоритмов;	Лекции; Лабораторные работы; Самостоятельная работа
12.навыками математического моделирования в криптографии;	Лекции; Лабораторные работы; Самостоятельная работа
13.криптографической терминологией;	Лекции; Лабораторные работы; Самостоятельная работа

14.использовать криптографические методы и средства защиты информации в автоматизированных системах;	Лекции; Лабораторные работы; Самостоятельная работа
15.основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;	Лекции; Лабораторные работы; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 6			
Дидактическая единица: Шифры			
1. Назначение и классификация шифров. Основные определения	0	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9
2. Шифр перестановки	0	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9
3. Шифр замены	0	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9
4. Шифры с открытым ключом	0	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9
5. Стандартные шифры	0	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9
Дидактическая единица: Криптоанализ			
6. Методы криптоанализа	0	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9
Дидактическая единица: Стандартные шифры			
7. Шифры DES, AES, ГОСТ	0	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9
Дидактическая единица: Приложения шифров			
8. Генерация псевдослучайных последовательностей	0	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9
9. Криптографическая идентификация и аутентификация	0	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 6				
Дидактическая единица: Шифры				
1. Частотные характеристики текстов	1	2	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	Частотные характеристики текстов
2. Шифр перестановки	1	2	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	Шифр перестановки

3. Шифр замены	1	2	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	Шифр замены
4. Шифры замены и перестановки	1	2	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	Шифры замены и перестановки
Дидактическая единица: Криптоанализ				
5. Криптоанализ классических шифров	1	2	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	Криптоанализ классических шифров
Дидактическая единица: Стандартные шифры				
6. Шифры DES, AES, ОСТ	1	4	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	Шифры DES, AES, ОСТ
Дидактическая единица: Приложения шифров				
7. Шифр с открытым ключом RSA	1	2	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	Шифр с открытым ключом RSA
8. Электорнная цифровая подпись RSA	1	2	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	Электорнная цифровая подпись RSA

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 6				
1	Курсовая работа	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	48	8
Курсовая работа: Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768				
2	Подготовка к занятиям	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	50	1
: Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768				
3	Подготовка к аттестации	1, 10, 11, 12, 13, 14, 15, 2, 3, 4, 5, 6, 7, 8, 9	15	2
Подготовка к аттестации: Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Социальные сети
Консультирование	e-mail
Контроль	Портал НГТУ
Размещение учебных материалов	Портал НГТУ

Таблица 5.2

Активные и интерактивные формы проведения занятий

№	Наименование активных форм	Коды формируемых компетенций
1	Проблемный метод	ПК.14; ПК.26;
Формируемые умения: з2. знать место криптографических методов в подсистемах информационной безопасности объекта защиты; у1. уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты; у2. уметь проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации		
Краткое описание применения: Решение поставленной задачи при известных ограничениях известными методами		
Подробная информация об использовании технологии приводится в "Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768"		

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Максимальный балл
Семестр: 6	
Лабораторная:	60
Контролирующие материалы (список вопросов) приводятся в "Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768"	
Курсовая работа:	
Контролирующие материалы (список вопросов) приводятся в "Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768"	
Экзамен:	40
Контролирующие материалы (список вопросов) приводятся в "Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768"	

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля		
		Защита Л/Р	Защита КП/КР	Экзамен
ПК.14	у2. уметь проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации	+	+	+
ПК.26	з2. знать место криптографических методов в подсистемах информационной безопасности объекта защиты	+	+	+
	у1. уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты	+	+	+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : курс лекций : учебное пособие для вузов по специальности 510200 "Прикладная математика и информатика" / О. Р. Лапонина ; под ред. В. А. Сухомлина. - М., 2005. - 604, [1] с. : ил., табл.

2. Осипян В. О. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян. - М., 2004. - 143 с.

3. Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 57, [1] с.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326

Дополнительная литература

1. Баричев С. Г. Основы современной криптографии : учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - М., 2002. - 175 с. : ил.

2. Кузьминов Т. В. Криптографические методы защиты информации / Т. В. Кузьминов ; отв. ред. В. А. Евстигнеев. - Новосибирск, 1998. - 185 с. : ил.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Минин И. В. Криптографические методы защиты информации : учебно-методическое пособие / И. В. Минин, О. В. Минин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2009. - 31, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000121807

2. Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768

8.2 Специализированное программное обеспечение

1 Windows
2 Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Используется при проведении лекционных занятий

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Исполльзуется при выполнении лабораторных работ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по дисциплине Криптографические методы защиты информации приведена в Таблице.

Таблица

Формируемые компетенции	Показатели сформированности компетенций (знания, умения, навыки)	Темы	Этапы оценки компетенций	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	Промежуточная аттестация (экзамен, зачет)
ПК.14/КА способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	у2. уметь проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств защиты информации	Генерация псевдослучайных последовательностей Криптоанализ классических шифров Криптографическая идентификация и аутентификация Методы криптоанализа Назначение и классификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES, AES, ОСТ Шифры замены и перестановки Шифры с открытым ключом Электорнная цифровая подпись RSA	Курсовая работа Отчет по лабораторной работе, разделы 1-5	Экзамен, вопросы 1-9
ПК.26/Э способность администрировать подсистему информационной безопасности автоматизированной системы	з2. знать место криптографических методов в подсистемах информационной безопасности объекта защиты	Генерация псевдослучайных последовательностей Криптоанализ классических шифров Криптографическая идентификация и аутентификация Методы криптоанализа Назначение и классификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES, AES, ОСТ Шифры замены и перестановки Шифры с открытым ключом Электорнная цифровая подпись RSA	Курсовая работа Отчет по лабораторной работе, разделы 1-5	Экзамен, вопросы10-18
ПК.26/Э	у1. уметь определять влияние криптографических методов на защищенность подсистем информационной безопасности объекта защиты	Генерация псевдослучайных последовательностей Криптоанализ классических шифров Криптографическая идентификация и аутентификация Методы криптоанализа Назначение и классификация шифров. Основные определения Стандартные шифры Частотные характеристики текстов Шифр замены Шифр	Курсовая работа Отчет по лабораторной работе, разделы...	Экзамен, вопросы 19-28

		перестановки Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES, AES, ОСТ Шифры замены и перестановки Шифры с открытым ключом Электорнная цифровая подпись RSA		

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 6 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ПК.14/КА, ПК.26/Э.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 6 семестре обязательным этапом текущей аттестации является курсовая работа. Требования к выполнению курсовой работы, состав и правила оценки сформулированы в паспорте курсовой работы.

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ПК.14/КА, ПК.26/Э, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт экзамена

по дисциплине «Криптографические методы защиты информации», 6 семестр

1. Методика оценки

Экзамен проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-28, задача выбирается из диапазона задач 1-10. В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы и задачи из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к экзамену по дисциплине «Криптографические методы защиты информации»

---

1. Шифры и шифрование. Основные понятия и определения
2. Зашифровать свою фамилию, имя и отчество, используя шифр Гронсфельда. В качестве ключа использовать свое имя

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

2. Критерии оценки

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки,
  оценка составляет *_10_ баллов.*
- Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные,
  оценка составляет *__20_ баллов.*
- Ответ на экзаменационный билет (тест) билет засчитывается на **базовом** уровне, если

студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи,
оценка составляет *_30_ баллов.*

- Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи,
оценка составляет _40_ *баллов.*

3. Шкала оценки

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы и задачи к** экзамену **по дисциплине «**Криптографические методы защиты информации**»**

1	Криптографическая защита информации. Классификация шифров. Требования к средствам криптографической защиты информации.
2	Шифры и шифрование. Основные понятия и определения
3	Шифры перестановки
4	Шифры замены
5	Шифр гаммирования
6	Шифр гаммирования с обратной связью
7	Совершенные, идеально стойкие, абсолютно стойкие шифры
8	Длина ключа и стойкость шифра
9	Фундаментальные ограничения криптографических преобразований
10	Проблемы массового использования шифров. Стандартные схемы и приемы реализации массовых шифров.
11	Стандартные шифры (DES, ГОСТ, AES).
12	Стандарт шифрования DES.
13	Режимы использования шифра DES
14	Стандарт шифрования ГОСТ 28147-89
15	Стандарт шифрования AES
16	Генераторы псевдослучайных чисел в шифровании
17	Основные подходы и методики криптоанализа.
18	Криптоанализ с использованием открытого текста.
19	Криптосистемы с открытым ключем. Принцип Шеннона. Основные особенности и характеристики криптосистем с открытым ключем
29	Структура системы секретной связи при использовании симметричных шифров и шифров с открытым ключом
21	Система Диффи-Хелмана
22	Шифр RSA

23	Шифр Эль Гаммаля
24	Гибридные криптосистемы
25	Основные проблемы криптографической защиты и способы их решения
26	Применение шифров для идентификации и аутентификации субъектов и данных. Хэш-функции. Электронно-цифровая подпись. Схемы цифровой подписи.
27	Отечественные стандарт хэш-функции ГОСТ Р 34.11-94
28	Отечественные стандарт шифрования с открытым ключом и электронно-цифровой подписи ГОСТ Р 34.10-94

ЗАДАЧИ К ЭКЗАМЕНУ

1. Зашифровать свою фамилию, имя и отчество, используя шифр простой перестановки.

2. Зашифровать свою фамилию, имя и отчество, используя шифр одиночной перестановки по ключу. В качестве ключа взять свое имя.

3. Зашифровать свою фамилию, имя и отчество, используя метод Полибия.
   В качестве алфавита взять буквы, включенные в ФИО.

4. Зашифровать свою фамилию, имя и отчество, используя шифр Гронсфельда. В качестве ключа использовать свое имя.

5. Зашифровать свою фамилию, имя и отчество, используя шифр Виженера. В качестве алфавита взять буквы, включенные в ФИО, а в качестве ключа использовать свое отчество.

6. Определить длину ключа в каждом из случаев: 0101 0101 0101 0101; 0000 0000 0000 0000; FEFE FEFA FEFE FEFA. Ключи даны в 16-ричной системе.

7. Для метода RSA и $p<20$, $q<20$ сформировать ключи «d» и «e».

8. Зашифровать открытый текст 1101011001101010110101 методом гаммирования, используя ключ 1011101011. Исходная информация и ключ даны в двоичной системе.

9. Зашифровать открытый текст 1101011001101010110101 методом гаммирования с обратной связью, используя ключ 1011101011 и блок размером 4 бита. Исходная информация и ключ даны в двоичной системе.

10. Определить, сколько различных электронных документов можно представить с помощью хэш-значений длиной 16 бит и 32бита.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт
курсовой работы

по дисциплине «Криптографические методы защиты информации», 6 семестр

1. **Методика оценки.**

Задание: Шифр Виженера.

Структура:1. Цель работы. 2. Постановка задачи. 3.Результаты выполнения. 4. Заключение. 5. Список литературы.

Этапы выполнения и защиты: в соответствии со структурой

Оцениваемые позиции: работа в целом.

2. **Критерии оценки.**

- работа считается **не выполненной,** если оценка составляет менее 49 баллов.
- работа считается выполненной **на пороговом** уровне, если оценка составляет 50-72 баллов.
- работа считается выполненной **на базовом** уровне, если оценка составляет 73-88 баллов.
- работа считается выполненной **на продвинутом** уровне, если _____, оценка составляет более 88 баллов.

3. **Шкала оценки.**

В общей оценке по дисциплине баллы за работы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Примерный перечень тем курсового проекта (работы).**

1. Шифр одиночной перестановка по ключу.
2. Шифр двойной перестановка по ключу.
3. Шифр перестановки с запретом записи.
4. Шифр перестановки на основе «магического» квадрата.
5. Шифр перестановки «по маршрутам».
6. Шифр перестановки с различными размерами блоков.
7. Шифр простой перестановки с изменением направления записи/чтения.
8. Шифры замены. Система Цезаря.
9. Шифры замены. Система Полибия.
10. Шифры замены. Простая замена.
11. Шифр Гронсфельда.
12. Шифр Виженера.
13. Шифр многоалфавитной замены.

14. Шифр монофонической замены.

15. Шифр гаммирования.

5. Перечень вопросов к защите курсового проекта (работы).

Вопросы для защиты курсового проекта по дисциплине
«Криптографические методы защиты информации»

Минимальное количество вопросов – 2, по одному из каждой части.

Часть 1

1.
1. Дайте определение шифра, ключа.
2. Чем шифрование отличается от кодирования.
3. Что такое тайнопись.
4. Для чего применяются шифры.
5. Что такое алфавит.
6. Какое значение имеет буква.
7. Что такое (k. –граммы.
8. Что такое индекс совпадения и как он вычисляется.
   Как в закодированном тексте выделить с помощью биграмм:
9. Символы (О,Е,А,И);
10. Символы (Ь,Ы).
11. Символ (Э);
12. Символы (С,Т);
13. Символ (Л);
14. Символ (Н);
15. Символы (О,В).

2.
1. Какие шифры называются симметричными.
2. Особенность секретной связи при использовании симметричных шифров.
3. Какие шифры называются перестановкой.
4. Определение функциональной эквивалентности шифров.
5. В чем заключается единственность шифра перестановки.
   Приведите схему перестановки:
6. простой;
7. одиночной по ключу;
8. двойной по ключу;
9. с запретом записи;
10. с использованием магических квадратов;
11. по «маршрутам»;
12. со сменой направления записи/чтения;
13. использующей разные размеры блоков;
14. повторной перестановки.
15. Как определить размер блока линейной перестановки для повторных перестановок.
16. В чем заключаются фундаментальные особенности шифров перестановки.
17. Что называется циклом или раундом при шифровании.
18. Что такое характеристическая функция ключа и для чего она может быть использована.
19. Какому шифру перестановки функционально эквивалентны остальные шифры перестановки.

3.
1. Как определяется стойкость шифра.
2. В каких единицах измеряется длина ключа.
3. В каких единицах измеряется стойкость шифра.
4. Что такое расстояние единственности.
5. В каких единицах измеряется переборная стойкость шифра.
6. В чем различие между длиной и размером ключа.
7. Что такое период ключа.
8. В чем заключаются фундаментальные особенности перестановки.
9. Приведите примеры чувствительности перестановки к специально подобранному тексту.
10. В чем заключается зависимости длины ключа перестановки от шифруемого текста.

11. В чем особенность шифрования перестановкой не полностью заполненного блока текста.
12. Какими способами можно повысить эффективность шифра перестановки.
13. Что такое защищенная кодировка и в чем ее смысл.
14. Как и в каких единицах измеряется переборная стойкость шифра.

4.
1. Какие шифры называются шифрами замены.
2. Опишите шифр:
а. Цезаря;
б. Полибия;
в. простой замены;
г. Гронсфельда;
д. Виженера.
3. Чем системы Цезаря, Полибия и простой замены отличаются от других шифров замены.
4. Приведите формулу общей математической модели шифров Цезаря, Гронсфелда, Виженера.
5. Какие шифры называются шифрами Бофора.
6. Какой шифр называется шифром Вернама.
7. Постройте собственный пример шифрования и расшифрования по формулам (4.2., отличающийся от приведенного в пособии.
8. Какой шифр называется шифром гаммирования, с какими известными шифрами и как он связан.
9. Что называется инфляцией алфавита.
10. В чем основная особенность шифра гаммирования.
11. Какой условие должно выполняться для обратимого шифрования композицией замен.
12. Какой алфавит называется входным (исходным) для шифра, а какой – выходным алфавитом.
13. Какие шифры называются одноалфавитными, моноалфавитными, полиалфавитными, многоалфавитными.
14. Как получить ключ шифра замены при шифровании перестановкой.
15. Частным случаем каких шифров является шифр перестановки.
16. Какой шифр называется шифром гаммирования с обратной связью.
17. Что общего у шифров монофонической замены, перестановки и гаммирования с обратной связью.
18. Как объединяются повторные применения шифров:
а. Цезаря;
б. Виженера;
в. простой замены и Виженера.

Часть 2.

5.
1. Размер блока и ключа шифра DES.
2. Размер блока и ключа шифра AES.
3. Размер блока и ключа шифра ГОСТ.
4. Режимы работы шифра DES.
5. Режимы работы шифра ГОСТ.
6. Количество базовых циклов шифрования в шифре DES.
7. Количество базовых циклов шифрования в шифре AES.
8. Количество базовых циклов шифрования в шифре ГОСТ.
9. Что называется имитовставкой в шифре ГОСТ.
10. Как определяется размер имитовставки.
11. Что называется синхропосылкой в шифре ГОСТ.
12. Что называется сетью Фейстейля.
13. Что называется SP-сетью.
14. Где в сообщении должна располагаться имитовставка шифра ГОСТ.
15. Какой шифр называется 3DES.

6.
1. Назначение и ограничения метода полного перебора.
2. Что называется переборным пространством.
3. Теоретическая оценка сокращения переборного пространства при поиске по образцу.
4. Чем отличается направленный случайный поиск от простого случайного поиска.
5. В каком случае при случайном поиске число просмотров будет минимальным.
6. В чем заключается метод проб и ошибок, с каким разделом математической статистики он связан.

7. Что называется «парадоксом дней рождения».
8. Каким требованиям (по Шеннону. должен отвечать «хороший» статистический метод криптоанализа.
9. Определите два основных класса методов криптоанализа.

В ответах на контрольные вопросы 10-16 дайте определение и опишите основные элементы для указанного в вопросе метода.

10. Метод вероятных слов.
11. Тест Казиски.
12. Метод «встречи посередине».
13. Метод линейного криптоанализа.
14. Метод дифференциального криптоанализа
15. Слайдовый метод.
16. Метод криптоанализа на связанных ключах.