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

Кафедра автоматизированных систем управления

“УТВЕРЖДАЮ”
ДИРЕКТОР ИСТР
д.соц.н. Осьмук Л. А.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Защита информации

Образовательная программа: 09.03.01 Информатика и вычислительная техника, профиль: Автоматизированные системы обработки информации и управления в социальной сфере

Курс: 4, семестр : 7

Институт социальных технологий и реабилитации,

		Семестр
№	**Вид деятельности**	**7**
1	Всего зачетных единиц (кредитов)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	64
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	18
8	Аттестация, час.	2
9	Консультации, час.	8
10	Самостоятельная работа, час.	80
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	контр.
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 09.03.01 Информатика и вычислительная техника

ФГОС введен в действие приказом №5 от 12.01.2016 г. , дата утверждения: 09.02.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 09.03.01 Информатика и вычислительная техника

Рабочая программа обсуждена на заседании кафедры

АСУ, протокол заседания кафедры №7 от 20.06.2017

Утверждена на совете института социальных технологий и реабилитации, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.т.н. Качальский В. Г.

Заведующий кафедрой:

профессор, д.т.н. Гриф М. Г.

Ответственный за образовательную программу:

заведующий кафедрой Гриф М. Г.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОПК.5 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; *в части следующих результатов обучения*:**
з5. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты
у12. уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе
у5. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств
у8. владеть персональным компьютером как средством управления информацией
***Компетенция ФГОС*: ПК.3 способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности; *в части следующих результатов обучения*:**
у4. уметь обосновывать принимаемые проектные решения
у9. владеть методами оценки трудоемкости программного проекта

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	Формы организации занятий
Защита информации	
ОПК.5.з5 знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	
1.	Лекции; Самостоятельная работа
ОПК.5.у12 уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе	
2.	Самостоятельная работа
ОПК.5.у5 уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	
3.	Лекции
ОПК.5.у8 владеть персональным компьютером как средством управления информацией	
4.	Лабораторные работы; Самостоятельная работа
ПК.3.у4 уметь обосновывать принимаемые проектные решения	
5.	Лекции
ПК.3.у9 владеть методами оценки трудоемкости программного проекта	
6.	Лекции

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 7			
Дидактическая единица: Понимание сути задачи			
1.	0	36	1, 3, 5, 6

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Понимание сути задачи				
1. Оранжевая книга	18	18	4	Подготовка а лаб.работе

Таблица 3.3

Темы для самостоятельного изучения	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Понимание сути задачи				
1. Шифрование данных	0	72	1, 2	Самостоятельная работа

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	Контрольные работы	1, 2, 4	8	0
: Быков С. В. Защита информации от утечки по каналам побочных электромагнитных излучений (ПЭИТ) : учебно-методическое пособие / С. В. Быков, В. А. Трушин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2008. - 41, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000084306				
2	Самостоятельное изучение теоретического материала	1, 2	80	8
Студент изучает темы, приведенные в таблице 3.3 : Денисов В. В. Защита информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Денисов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000176937. - Загл. с экрана.				

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
Консультирование	e-mail
Контроль	Чат
Размещение учебных материалов	Среда электронного обучения НГТУ

Таблица 5.2

Активные и интерактивные формы проведения занятий

№	Наименование активных форм
1	Лекция в форме дискуссии:Контрольные суммы
Краткое описание применения:	
Подробная информация об использовании технологии приводится в "Денисов В. В. Защита информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Денисов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000176937. - Загл. с экрана."	
2	Лекция в форме дискуссии:Контрольные суммы
Краткое описание применения:	
Подробная информация об использовании технологии приводится в "Быков С. В. Защита информации от утечки по каналам побочных электромагнитных излучений (ПЭИТ) : учебно-методическое пособие / С. В. Быков, В. А. Трушин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2008. - 41, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000084306"	

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	Мин. балл	Максимальный балл
Семестр: 7		
Самостоятельное изучение теоретического материала:	0	
Лабораторная:	40	80
Контрольные работы:	40	80
Экзамен:	40	90

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	Контр. раб.	Экзамен
ОПК.5	з5. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты			+
	у12. уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе		+	
	у5. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств			+
	у8. владеть персональным компьютером как средством управления информацией	+		
ПК.3	у4. уметь обосновывать принимаемые проектные решения			+

	у9. владеть методами оценки трудоемкости программного проекта			+

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

7. Литература

Основная литература

1. Галицкий А. В. Защита информации в сети - анализ технологий и синтез решений / Галицкий, А. В. Рябко С. Д., Шаньгин В. Ф. - М., 2004. - 613 с. : ил.

2. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. - М., 2001. - 376 с.

Дополнительная литература

1. ГОСТ Р51188-99 Защита информации. Испытание программных средств на наличие компьютерных вирусов [Электронный ресурс] : типовое руководство. - Б. м., [2001]. - 1 дискета

2. Завгородний В. И. Комплексная защита информации в компьютерных сетях : Учеб. пособие для вузов. - М., 2001. - 263 с.

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. Денисов В. В. Защита информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Денисов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000176937. - Загл. с экрана.

2. Быков С. В. Защита информации от утечки по каналам побочных электромагнитных излучений (ПЭИТ) : учебно-методическое пособие / С. В. Быков, В. А. Трушин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2008. - 41, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000084306

8.2 Специализированное программное обеспечение

1 Microsoft Windows

2 Microsoft Office

9. Материально-техническое обеспечение

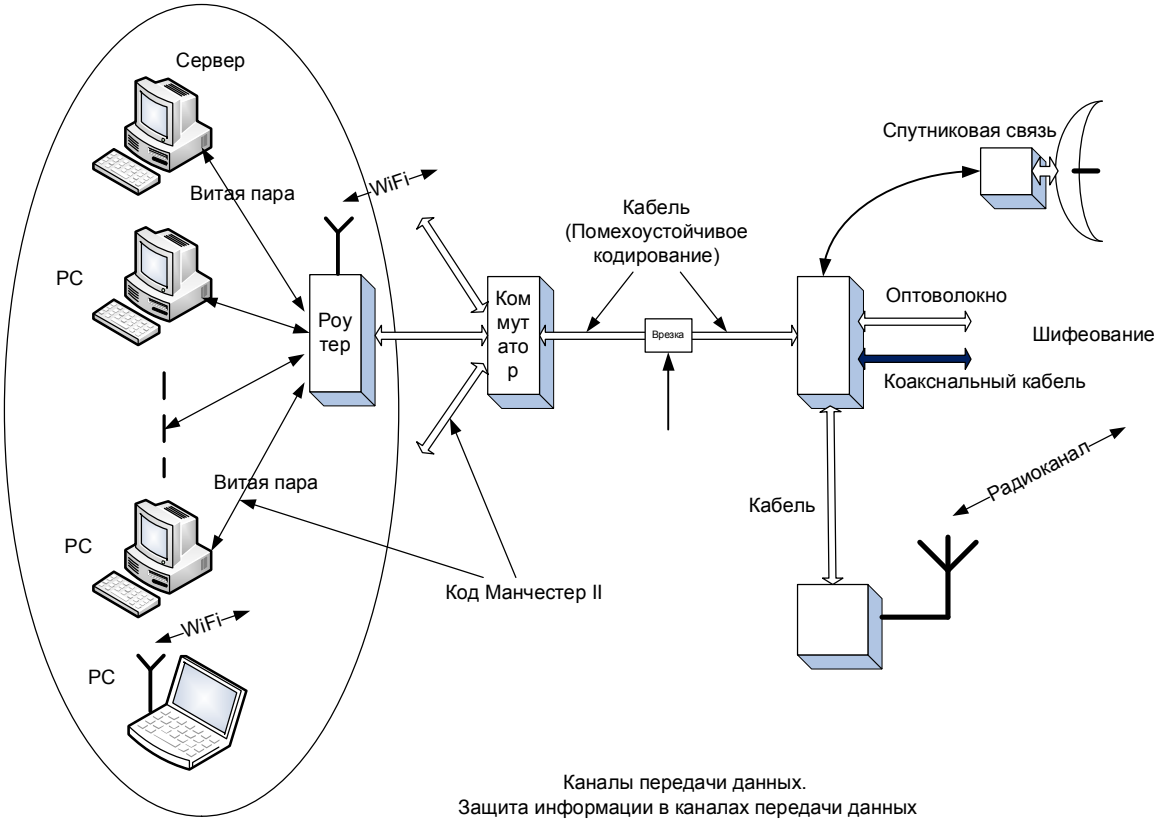
Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Компьютеры объединены в локальную сеть с выходом в Internet

Вопросы на экзамене по курсу «Защита информации» 2015г.

1	Обзор основных угроз информационной безопасности.
2	Системы идентификации и аутентификации пользователей
3	Оценка надежность систем в соответствии с «Оранжевой книгой»
4	Основные элементы политики безопасности в соответствии с «Оранжевой книгой»
5	Критерии оценки надежных компьютерных систем. в соответствии с «Оранжевой книгой»
6	Шифрование методом замены (подстановки). Одноалфавитная подстановка
7	Шифрование методом замены (подстановки). Многоалфавитная одноконтурная обыкновенная подстановка.
8	Многоалфавитная одноконтурная монофоническая подстановка.
9	Шифрование методом перестановки. Простая перестановка.
10	Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам
11	Шифрование методом гаммирования.
12	Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.
13	Организационные проблемы криптозащиты
14	Стандарт шифрования данных Data Encryption Standard (DES), Принцип построения и обобщенный алгоритм
16	Отечественный стандарт шифрования данных. Обозначения, Параметры и сравнение с DES
16	Отечественный стандарт шифрования данных. Блок-схема цикла щифрования
17	Отечественный стандарт шифрования данных. Режим гаммирования и с обратной связью
18	Отечественный стандарт шифрования данных. Выработка имитовставки.
19	Концепция криптосистемы с открытым ключом. Однонаправленные функции

20	Система распределения ключей Диффи-Хеллмана, применение.
21	Криптографическая защиты информации с известным ключом RSA.
22	Электронная подпись в системах с открытым ключом
23	Проблема аутентификации данных и электронная цифровая подпись
24	Однонаправленные хэш-функции, основы построения хэш-функций
25	Однонаправленные хэш-функции на основе симметричных блочных алгоритмов
26	Четыре схемы безопасного хэширования
27	Отечественный стандарт хэш-функции
28	Отечественный стандарт цифровой подписи
29	Защита программного продукта от несанкционированного копирования, Методы защиты дискеты.
30	Защита программного продукта от несанкционированного копирования, Методы защиты CD.
31	Введение ограничений на использование программного обеспечения
32	Методы взлома и способам защиты от них
33	Отладчики и методы защиты от них
34	Дизассемблеры и дамперы и защита от них
35	Программы с потенциально опасными последствиями, вирус
36	Люк, Троянский конь, Логическая бомба
37	Программные закладки. Обзор и методы защиты
38	Межсетевые экраны. Пакетные фильтры и серверы прикладного уровня
39	Каналы передачи данных. Защита информации в каналах передачи данных.



Каналы передачи данных.
Защита информации в каналах передачи данных

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

Кафедра автоматизированных систем управления

“УТВЕРЖДАЮ”
ДИРЕКТОР ИСТР
д.соц.н., профессор Л.А. Осьмук
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации

Образовательная программа: 09.03.01 Информатика и вычислительная техника, профиль: Автоматизированные системы обработки информации и управления в социальной сфере

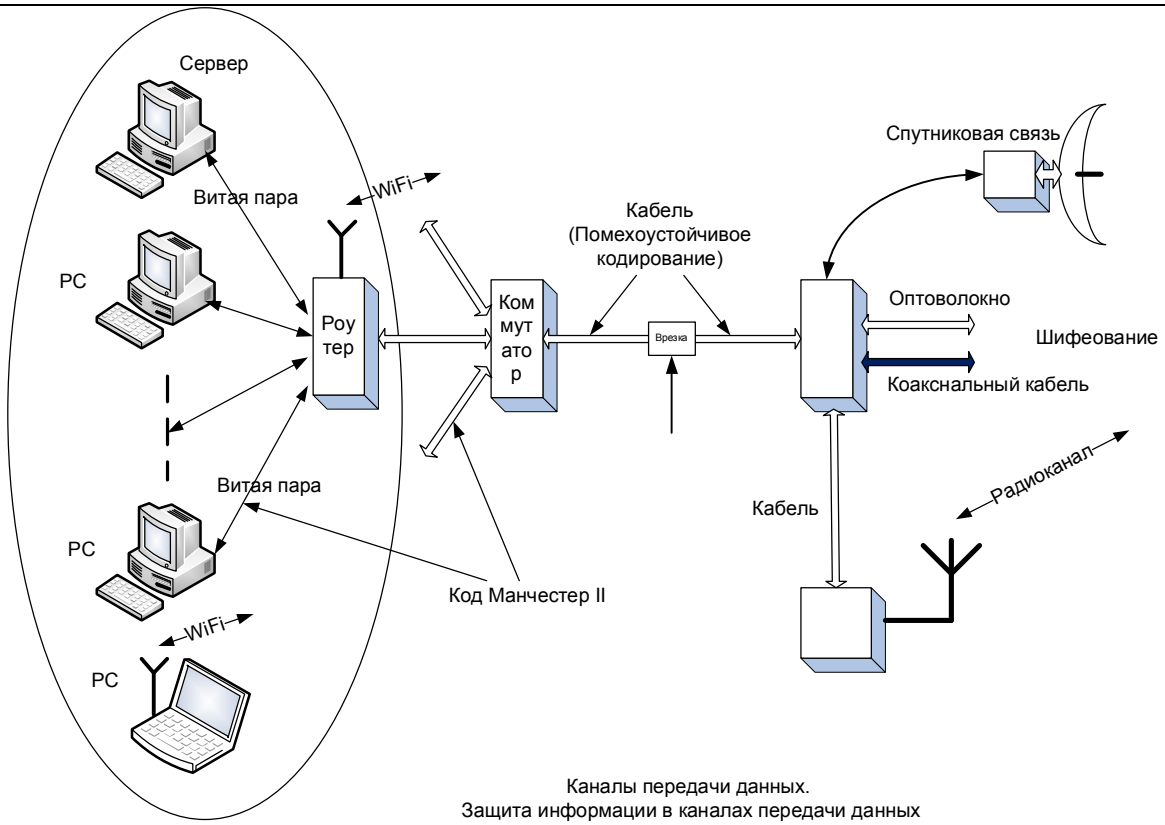
Новосибирск 2017

Вопросы на экзамене по курсу «Защита информации» 2015г.

1	Обзор основных угроз информационной безопасности.
2	Системы идентификации и аутентификации пользователей
3	Оценка надежность систем в соответствии с «Оранжевой книгой»
4	Основные элементы политики безопасности в соответствии с «Оранжевой книгой»
5	Критерии оценки надежных компьютерных систем. в соответствии с «Оранжевой книгой»
6	Шифрование методом замены (подстановки). Одноалфавитная подстановка
7	Шифрование методом замены (подстановки). Многоалфавитная одноконтурная обыкновенная подстановка.
8	Многоалфавитная одноконтурная монофоническая подстановка.
9	Шифрование методом перестановки. Простая перестановка.
10	Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам
11	Шифрование методом гаммирования.
12	Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.
13	Организационные проблемы криптозащиты
14	Стандарт шифрования данных Data Encryption Standard (DES), Принцип построения и обобщенный алгоритм
16	Отечественный стандарт шифрования данных. Обозначения, Параметры и сравнение с DES
16	Отечественный стандарт шифрования данных. Блок-схема цикла щифрования

17	Отечественный стандарт шифрования данных. Режим гаммирования и с обратной связью
18	Отечественный стандарт шифрования данных. Выработка имитовставки.
19	Концепция криптосистемы с открытым ключом. Однонаправленные функции
20	Система распределения ключей Диффи-Хеллмана, применение.
21	Криптографическая защиты информации с известным ключом RSA.
22	Электронная подпись в системах с открытым ключом
23	Проблема аутентификации данных и электронная цифровая подпись
24	Однонаправленные хэш-функции, основы построения хэш-функций
25	Однонаправленные хэш-функции на основе симметричных блочных алгоритмов
26	Четыре схемы безопасного хэширования
27	Отечественный стандарт хэш-функции
28	Отечественный стандарт цифровой подписи
29	Защита программного продукта от несанкционированного копирования, Методы защиты дискеты.
30	Защита программного продукта от несанкционированного копирования, Методы защиты CD.
31	Введение ограничений на использование программного обеспечения
32	Методы взлома и способам защиты от них
33	Отладчики и методы защиты от них
34	Дизассемблеры и дамперы и защита от них
35	Программы с потенциально опасными последствиями, вирус

36	Люк, Троянский конь, Логическая бомба
37	Программные закладки. Обзор и методы защиты
38	Межсетевые экраны. Пакетные фильтры и серверы прикладного уровня
39	Каналы передачи данных. Защита информации в каналах передачи данных.

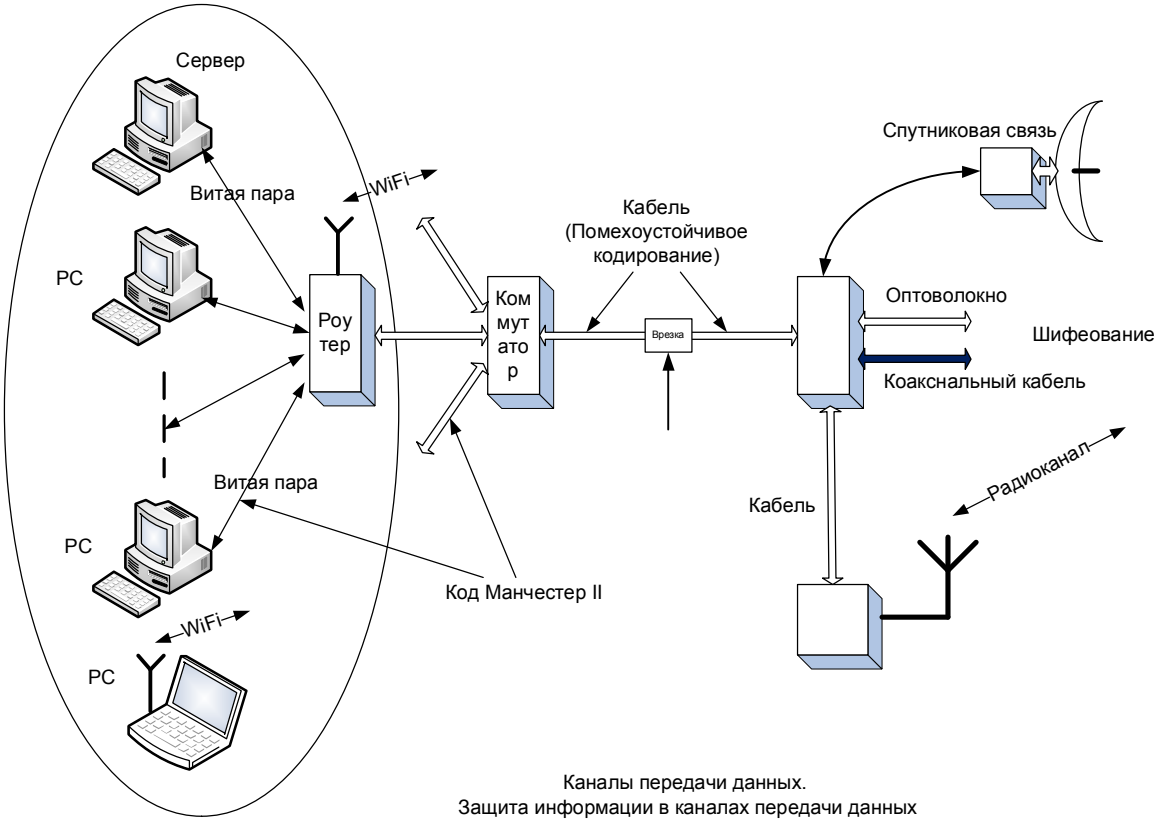


Каналы передачи данных.
Защита информации в каналах передачи данных

Вопросы на экзамене по курсу «Защита информации» 2015г.

1	Обзор основных угроз информационной безопасности.
2	Системы идентификации и аутентификации пользователей
3	Оценка надежность систем в соответствии с «Оранжевой книгой»
4	Основные элементы политики безопасности в соответствии с «Оранжевой книгой»
5	Критерии оценки надежных компьютерных систем. в соответствии с «Оранжевой книгой»
6	Шифрование методом замены (подстановки). Одноалфавитная подстановка
7	Шифрование методом замены (подстановки). Многоалфавитная одноконтурная обыкновенная подстановка.
8	Многоалфавитная одноконтурная монофоническая подстановка.
9	Шифрование методом перестановки. Простая перестановка.
10	Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам
11	Шифрование методом гаммирования.
12	Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.
13	Организационные проблемы криптозащиты
14	Стандарт шифрования данных Data Encryption Standard (DES), Принцип построения и обобщенный алгоритм
16	Отечественный стандарт шифрования данных. Обозначения, Параметры и сравнение с DES
16	Отечественный стандарт шифрования данных. Блок-схема цикла щифрования
17	Отечественный стандарт шифрования данных. Режим гаммирования и с обратной связью
18	Отечественный стандарт шифрования данных. Выработка имитовставки.
19	Концепция криптосистемы с открытым ключом. Однонаправленные функции

20	Система распределения ключей Диффи-Хеллмана, применение.
21	Криптографическая защиты информации с известным ключом RSA.
22	Электронная подпись в системах с открытым ключом
23	Проблема аутентификации данных и электронная цифровая подпись
24	Однонаправленные хэш-функции, основы построения хэш-функций
25	Однонаправленные хэш-функции на основе симметричных блочных алгоритмов
26	Четыре схемы безопасного хэширования
27	Отечественный стандарт хэш-функции
28	Отечественный стандарт цифровой подписи
29	Защита программного продукта от несанкционированного копирования, Методы защиты дискеты.
30	Защита программного продукта от несанкционированного копирования, Методы защиты CD.
31	Введение ограничений на использование программного обеспечения
32	Методы взлома и способам защиты от них
33	Отладчики и методы защиты от них
34	Дизассемблеры и дамперы и защита от них
35	Программы с потенциально опасными последствиями, вирус
36	Люк, Троянский конь, Логическая бомба
37	Программные закладки. Обзор и методы защиты
38	Межсетевые экраны. Пакетные фильтры и серверы прикладного уровня
39	Каналы передачи данных. Защита информации в каналах передачи данных.



Каналы передачи данных.
Защита информации в каналах передачи данных

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

Кафедра автоматизированных систем управления

“УТВЕРЖДАЮ”
ДИРЕКТОР ИСТР
к.т.н. Птушкин Г. С.
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ
Защита информации

Образовательная программа: 09.03.01 Информатика и вычислительная техника

Институт социальных технологий и реабилитации

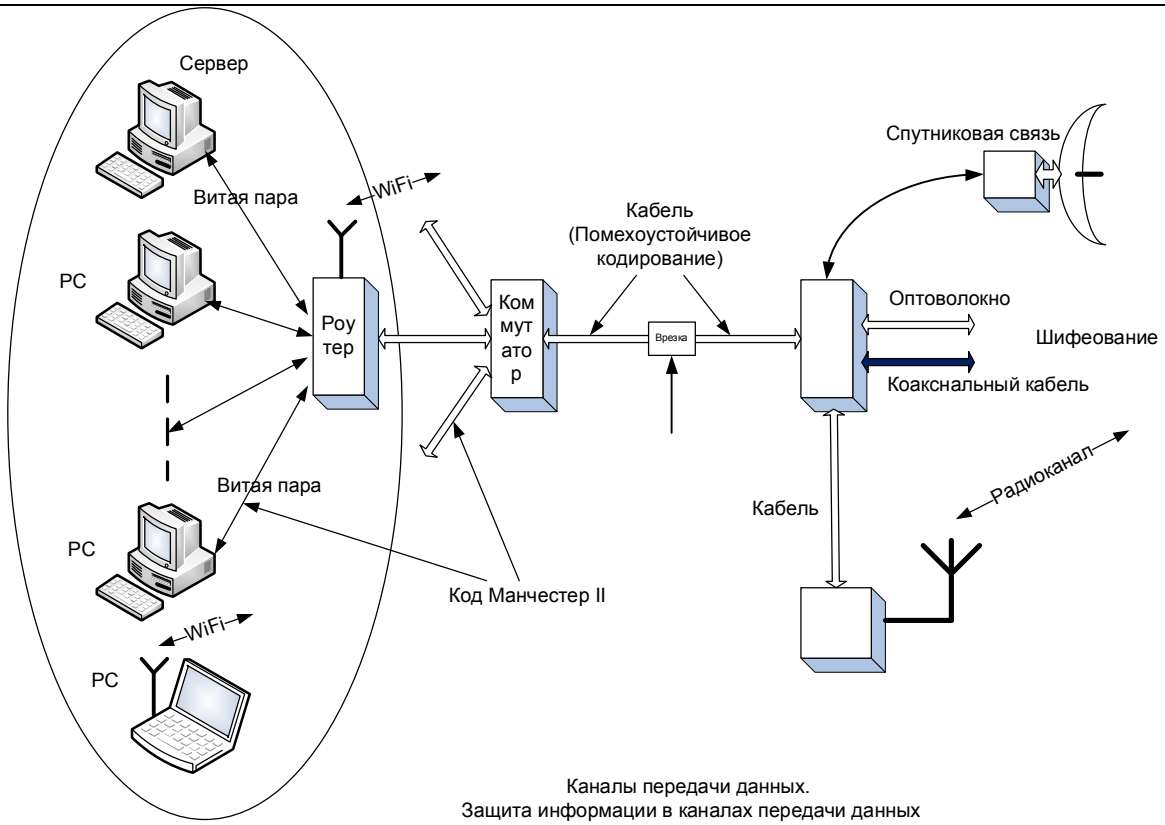
Новосибирск 2015

Вопросы на экзамене по курсу «Защита информации» 2015г.

1	Обзор основных угроз информационной безопасности.
2	Системы идентификации и аутентификации пользователей
3	Оценка надежность систем в соответствии с «Оранжевой книгой»
4	Основные элементы политики безопасности в соответствии с «Оранжевой книгой»
5	Критерии оценки надежных компьютерных систем. в соответствии с «Оранжевой книгой»
6	Шифрование методом замены (подстановки). Одноалфавитная подстановка
7	Шифрование методом замены (подстановки). Многоалфавитная одноконтурная обыкновенная подстановка.
8	Многоалфавитная одноконтурная монофоническая подстановка.
9	Шифрование методом перестановки. Простая перестановка.
10	Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам
11	Шифрование методом гаммирования.
12	Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.
13	Организационные проблемы криптозащиты
14	Стандарт шифрования данных Data Encryption Standard (DES), Принцип построения и обобщенный алгоритм
16	Отечественный стандарт шифрования данных. Обозначения, Параметры и сравнение с DES
16	Отечественный стандарт шифрования данных. Блок-схема цикла щифрования

17	Отечественный стандарт шифрования данных. Режим гаммирования и с обратной связью
18	Отечественный стандарт шифрования данных. Выработка имитовставки.
19	Концепция криптосистемы с открытым ключом. Однонаправленные функции
20	Система распределения ключей Диффи-Хеллмана, применение.
21	Криптографическая защиты информации с известным ключом RSA.
22	Электронная подпись в системах с открытым ключом
23	Проблема аутентификации данных и электронная цифровая подпись
24	Однонаправленные хэш-функции, основы построения хэш-функций
25	Однонаправленные хэш-функции на основе симметричных блочных алгоритмов
26	Четыре схемы безопасного хэширования
27	Отечественный стандарт хэш-функции
28	Отечественный стандарт цифровой подписи
29	Защита программного продукта от несанкционированного копирования, Методы защиты дискеты.
30	Защита программного продукта от несанкционированного копирования, Методы защиты CD.
31	Введение ограничений на использование программного обеспечения
32	Методы взлома и способам защиты от них
33	Отладчики и методы защиты от них
34	Дизассемблеры и дамперы и защита от них
35	Программы с потенциально опасными последствиями, вирус

36	Люк, Троянский конь, Логическая бомба
37	Программные закладки. Обзор и методы защиты
38	Межсетевые экраны. Пакетные фильтры и серверы прикладного уровня
39	Каналы передачи данных. Защита информации в каналах передачи данных.



Каналы передачи данных.
Защита информации в каналах передачи данных