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

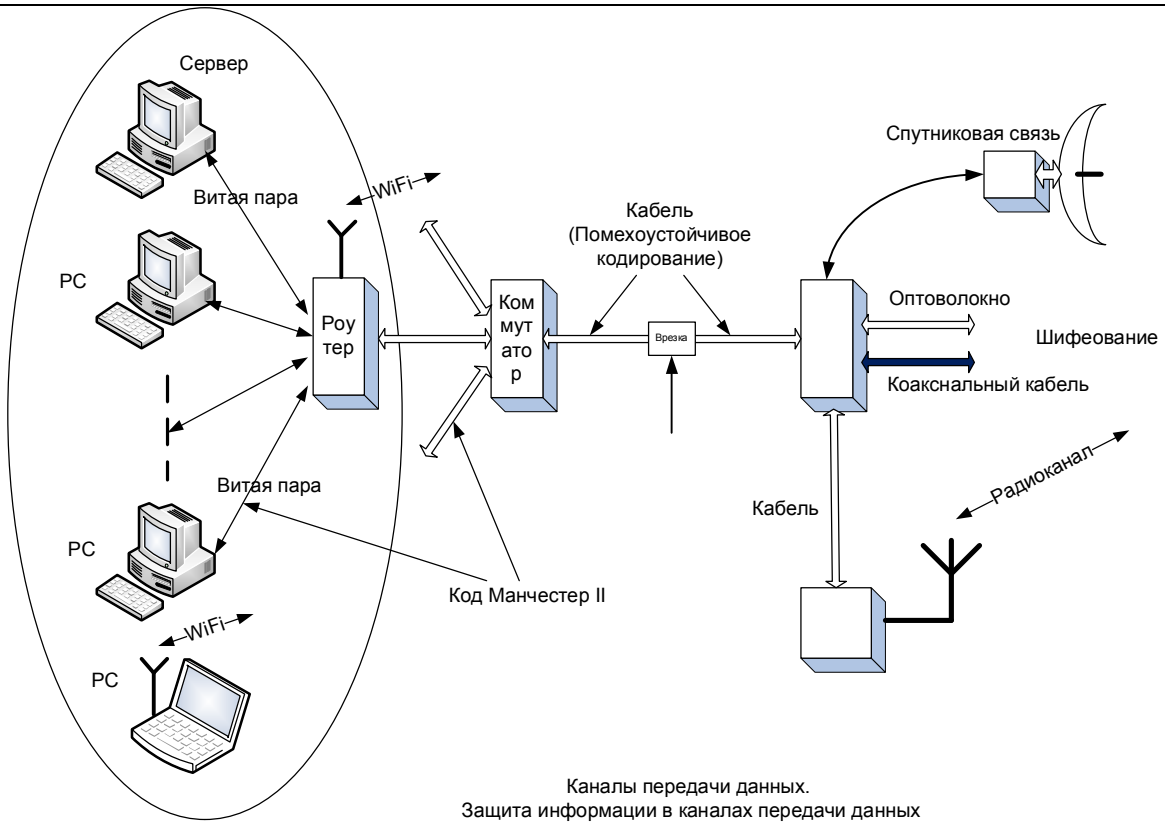
Новосибирск 2015

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