# Оценочные материалы для промежуточной аттестации по дисциплине

*Основы защиты информации*
*7 семестр*

| | |
|---|---|
| Код, направление подготовки | 09.03.04 |
| Направленность (профиль) | Программная инженерия |
| Форма обучения | очная |
| Кафедра-разработчик | Автоматики и компьютерных систем |
| Выпускающая кафедра | Автоматики и компьютерных систем |

## Типовые задания для контрольной работы:

Варианты контрольной работы:

Вариант 1:

1. Дать определение компьютерного преступления.

2. Вредоносное ПО.

3. Принципы и применение ассиметричных алгоритмов шифрования.

Вариант 2:

1. Классификация компьютерных преступлений.

2. Иерархический подход к построению политики безопасности.

3. Принципы и применение симметричных блочных алгоритмов шифрования.

Вариант 3:

1. Организационно – административное обеспечение безопасности.

2. Виды угроз.

3. Принципы и применение симметричных потоковых алгоритмов шифрования.

Вариант 4:

1. Инженерно-техническое обеспечение безопасности.

2. Стандарт безопасности «Оранжевая книга».

3. Принципы и применение циклических алгоритмов шифрования.

## Типовые вопросы к экзамену/зачету/зачету с оценкой:

1. Законодательные и правовые аспекты защиты информации. Актуальность проблематики защиты информационных ресурсов.
2. Информация и информационные ресурсы. Компьютерные преступления.
3. Основные законы, регламентирующие законодательство в области защиты информации. Правовая защита ПО.
4. Источники и формы атак на информацию. Классификация источников и форм атак на информационные ресурсы.
5. Наблюдение за каналами связи. Перехват побочных излучений. Задержка, изменение, подмена сообщений.
6. Способы получения парольной информации и прав доступа. Уязвимость ОС. Компьютерные вирусы. Включение разработчиком в программное обеспечение недокументированных функций.
7. Определение политики безопасности. Цели информационной безопасности.
8. Уровни безопасности. Реализация политики безопасности.
9. Реализация организационных и технических мер.
10. Стандарты безопасности. Роль стандартов. «Оранжевая книга».
11. Классы безопасности. Критерии оценки защищенности информационных систем.
12. Международный стандарт ISO/IEC 15408 и его российский аналог ГОСТ Р ИСО/МЭК 15408. Международный стандарт информационной безопасности ISO 17799. Стандарт ITU-T Recommendation X.805.
13. Криптографические протоколы. Криптология, криптография и криптоанализ. Основные понятия криптологии.
14. Стойкость, защищенность, имитостойкость, аутентичность. Стеганография. Подстановочные и перестановочные шифры. Элементы криптографических протоколов.
15. Смысл протоколов. Элементы криптосистем. Виды протоколов.
16. Симметричные криптосистемы. Блочные шифры. Модель криптосистемы с секретным ключом.
17. Описание блочных алгоритмов DES, ГОСТ.
18. Стандарт шифрования AES. Режимы применения блочных шифров.
19. Симметричные криптосистемы. Потоковые шифры. Блок-схема поточного шифратора.
20. Синхронные и самосинхронизирующиеся поточные криптоалгоритмы. Принципы построения.
21. Стандарт безопасности GSM. Описание потоковых алгоритмов A5, RC4.
22. Асимметричные криптосистемы. Модель криптосистемы с открытым ключом. Однонаправленные преобразования.
23. Криптосистема Эль-Гамаля. Открытое распределение ключей, система Диффи и Хеллмана.
24. Система Ривеста-Шамира-Адлемана (RSA). Криптосистемы Меркля-Хеллмана и Хора-Ривеста.
25. Требования к системам защиты информации. Общие требования. Организационные требования. Требования к техническому обеспечению. Требования к программному обеспечению. Требования по применению способов, методов и средств защиты. Требования к документированию.