Экзаменационная программа по предмету

«Защита информации в телекоммуникациях»

«Радиотехника, электроника и телекоммуникации»,
4 курс, бакалавриат.

Количество студентов - 8.

Тип экзамена
ПИСЬМЕННЫЙ ЭКЗАМЕН (офлайн).

письменный ответ на вопросы билета в системе ИС Univer (3 вопроса).

Платформа проведения экзамена: **ИС Univer**
Форма проведения экзамена: **Стандартный**
Вид экзамена: **Письменный**

Регламент
экзамен проводится в системе ИС Univer согласно расписанию,
Вкладка «Расписание экзаменов».

Объем - 3 часа по 3 вопроса. Общая база вопросов включает от 15 до 45 вопросов по кредитам предмета. Вопросы загружаются в анкету ИС Univer и отправляются в ИС Univer, закрепленную за учебными группами.

Система автоматически проверяет уникальность текста. Более 50% по любым вопросам = летний семестр. Осмотр проводят специалисты отдела. Экзаменатор оценивает соответствие ответов студента вопросам билета.

Экзаменатор закрывает форму сертификации ИС Univer
путем ручного перевода баллов ИС Univer
в течение 48 часов после письменного экзамена.

Правила и критерии оценки

Политика оценки и сертификации	**Суммарная оценка:** **Итоговая оценка** **Ответы:** 1-вопрос + 2- вопрос + 3- вопрос = 100 % Ниже приведены проценты: 95 – 100%: A 90 – 94%: A- 85 – 89%: B+ 80 – 84%: B 75 – 79%: B- 70 – 74%: C+ 65 – 69%: C 60 – 64%: C- 55 – 59%: D+ 50 – 54%: D- 0 – 49%: F

Список рекомендуемой литературы

1. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для вузов.- М.: Академия, 2005.- 254, [2] с.
2. Молдовян, А. А. и др. Криптография: Учеб..- СПб.: Лань, 2001.- 218, [6] с.
3. Нечаев, В.И. Элементы криптографии: (Основы теории защиты информации).- М.: Высш. шк., 1999.- 108, [1] с
4. Беляев А.В. Курс лекций по «Методы и средства защиты информации». http://citforum.ru/internet/infsecure/index.shtml
5. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000..
6. Домарев, В.В. Защита информации и безопасность компьютерных систем /.- Науч.-попул. изд.- Киев: СОФТ, 1999.- 453, [26] с
7. Галочкин, А.И. Введение в теорию чисел: Учеб. пособие - 2-е изд.- М.: МГУ, 1995.- 158, [2] с

Доступно онлайн:

8. Домашние задания и дополнительные учебные материалы по разделу УМКД сайта univer.kaznu.kz доступны на вашей странице.

Интернет-ресурсы

9. https://refdb.ru/look/1214614.html - Лекции по теме «Основы информационной безопасности».
10. http://www.4stud.info/networking/network-security.html Основы сетевой безопасности. Как объект защиты сети

Список основных тем экзаменационных вопросов

1. Общее понятие информационной безопасности, краткая история ее развития. Основные составляющие информационной безопасности
2. Ақпараттық қауіпсіздіктің заманауи стандарттары
3. Угрозы безопасности. Классификация опасностей.
4. Таблицы шифрования. Подстановочные шифры. Двойная замена.
5. Сервисы и механизмы безопасности. Протоколы связи на сетевом уровне.
6. Таблицы шифрования Trisemus. Система шифрования Виженера
7. Двойная площадь Уитстона. Шифр Биграма Playfair
8. Классификация сетевых атак. Категории атак и их определения, условия их осуществления. Механизм атаки
9. Криптографические механизмы защиты. Основные задачи и понятия криптографии. Принципы криптографической защиты информации.
10. Элементы теории чисел. НОД и сравнение. Теоремы Ферма и Эйлера для решения криптографических задач.
11. Симметричное и асимметричное шифрование в задачах защиты информации.
12. Криптосистема без передачи ключей. Решение проблем в криптосистеме без передачи ключа
13. Законодательные меры защиты в Республике Казахстан.
14. Принцип создания систем шифрования с открытым ключом. Алгоритм защиты информации с открытым ключом RSA
15. Алгоритмы цифровой подписи.
16. Сертификаты безопасности. Типы сертификатов безопасности.
17. Канальная сегментация сетей. Использование технологии VLAN для создания подсетей. Типичная топология сети с использованием VLAN.
18. Технологии межсетевого экрана. Основные понятия сетевых технологий (стек протоколов, состояния соединения TCP). Классификация брандмауэров
19. Туннельные технологии. Протоколы канального уровня. Семейство протоколов IPSec.
20. SIEM: анализ систем IBM QRadar, McAfee ESM, Cisco MARS