МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
РГП на ПХВ «Евразийский Национальный университет имени Л.Н. Гумилева»

Кафедра «Информатика и информационная безопасность»

УТВЕРЖДАЮ
Проректор по учебной работе
РГП на ПХВ «Евразийский Национальный университет имени Л.Н.Гумилева»
А.Молдажанова
_____ 2016 г.

ПРОГРАММА
дисциплин для поступающих по специальности
6М100200–Системы информационной безопасности

Обсуждена на заседании кафедры «Информатика и информационная безопасность»

Протокол №_11_ от «_8_» __06____ 2016 г.

Заведующая кафедрой Ж.Сауханова

Декан факультета Ж.Нурбекова

Астана 2016 г.

ДИСКРЕТНАЯ МАТЕМАТИКА

1. Множества. Элементы и множества. Сравнение множеств.
2. Мощность конечного множества. Операции над множествами.
3. Свойства операций над множествами
4. Элементарные булевы функции. Функции алгебры логики. Существенные и несущественные переменные
5. Булевы функции. Алгебра булевых функций.
6. Совершенные нормальные формы. Минимальные дизъюнктивные формы.
7. Сокращенные дизъюнктивные формы.
8. Алфавит языка логики высказываний
9. Синтаксис языка логики высказываний
10. Семантика языка логики высказываний
11. Связь с естественным языком
12. Выполнимые, общезначимые и нейтральные формулы
13. Алфавит языка логики предикатов
14. Синтаксис языка логики предикатов
15. Подстановка и конкретизация
16. Комбинаторика. Перестановки
17. Размещения
18. Перестановки
19. Алгоритм Фано
20. Алгоритм Хаффмена
21. Кодирование с минимальной избыточностью. Минимизация длины кода сообщения
22. Помехоустойчивое кодирование. Кодирование с исправлением ошибок
23. Помехоустойчивое кодирование. Код Хэмминга для исправления одного замещения
24. Графы. Основное определение. Смежность.
25. Элементы графов. Подграфы. Маршруты, цепи, циклы
26. Способы представления графа.
27. Графы. Алгоритм Флойда
28. Графы. Алгоритм Дейкстры
29. Задача коммивояжера
30. Раскраска графов

ОРГАНИЗАЦИЯ ОПЕРАЦИОННЫХ СИСТЕМ

1. Процессы
2. Адресные пространства
3. Файлы
4. Ввод-вывод данных
5. Оболочка операционной системы
6. Системные вызовы
7. Потоки
8. Реализация потоков в ядре
9. Реализация потоков в пользовательском пространстве
10. Критические области, взаимное исключение с активным ожиданием

11. Семафоры, мьютексы, мониторы
12. Память без использования абстракций
13. Абстракция памяти: адресные пространства
14. Виртуальная память
15. Алгоритмы замещения страниц
16. Сегментация
17. Файловые системы. Файлы. Каталоги
18. Реализация файловой системы
19. Взаимоблокировка
20. Мультипроцессоры
21. Механизмы защиты
22. Аутентификация
23. Использование дефектов программного кода
24. Вредоносные программы
25. Средства защиты
26. Инсайдерские атаки
27. Файловая система UNIX
28. Стандартная система UNIX
29. Структура ядра Linux
30. Windows операционная система

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1. Подстановочные шифры
2. Перестановочные шифры
3. Алгоритм Data Encryption Standard (DES)
4. Алгоритм Advanced Encryption Standard (AES)
5. Протокол обмена ключами Диффи-Хеллмана
6. Задача Диффи-Хеллмана и задача дискретного логарифмирования
7. Криптосистема RSA (учебный вариант)
8. Криптосистема Рабина (учебный вариант)
9. Криптосистема Эль-Гамаля (учебный вариант)
10. Криптографические хэш-функции
11. Асимметричные методы I: цифровые подписи
12. Асимметричные методы II: защита целостности данных без идентификации источника
13. Основные понятия аутентификации
14. Аутентификация с помощью пароля
15. Обмен аутентичными ключами с помощью асимметричной криптографии
16. Типичные атаки на протоколы аутентификации
17. Системы аутентификации с помощью службы каталогов
18. Аутентификация в криптографии с открытым ключом
19. Битовая стойкость алгоритма RSA
20. Битовая стойкость алгоритма Рабина
21. Битовая стойкость криптосистемы Эль-Гамаля
22. Битовая стойкость дискретного логарифма
23. Основные методы аутентификации
24. Обмен аутентичными ключами с помощью асимметричной криптографии
25. Протоколы аутентификации для обеспечения безопасности в Internet
26. Протокол удаленной регистрации SSH

В экзаменационные билеты дополнительно будут включены задачи по указанным дисциплинам

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Яблонский С.В. Введение в дискретную математику. – М.: Высш. шк., 2003. – 384 с.
2. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по дискретной математике. – М.: ФИЗМАТЛИТ, 2005. – 416 с.
3. Судоплатов С.В., Овчинникова Е.В. Элементы дискретной математики. – М.: ИНФРА-М; Новосибирск: НГТУ, 2003. – 280 с.
4. Новиков Ф.А. Дискретная математика для программистов. – СПб.: Питер, 2001. – 304 с.
5. Виленкин Н.Я. Комбинаторика. – М.: Наука, 1969.
6. Марченков С.С. Булевы функции. — М.: ФИЗМАТЛИТ, 2002.— 72 с.
7. Шабунин Л.В. Элементы комбинаторики. – Чебоксары: ЧГУ, 2003.
8. Завгородний, В.И. Комплексная защита информации в компьютерных системах : учебное пособие для вузов / В.И. Завгородний. – М. : Логос, 2001. – 264 с.
9. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М.
10. Теоретические основы компьютерной безопасности : учебное пособие для вузов/ П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. – М. : Радио и связь, 2000. – 192 с.
11. Грушо, А.А. Теоретические основы защиты информации / А.А. Грушо, Е.Е. Тимонина. – М. : Яхтсмен, 1996. – 192 с.
12. Жельников, В.Г. Криптография от папируса до компьютера / В.Г. Жельников. – М. : Dore Print, 1999. – 214 с.
13. Баричев, С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М. : Горячая линия – Телеком, 2001. – 121 с.
14. Олифер В. Г. Сетевые операционные системы : учебное пособие для вузов по направлению подготовки дипломированных специалистов "Информатика и вычислительная техника" / В. Г. Олифер, Н. А. Олифер. - СПб. [и др.], 2007. - 538 с. : ил. - Рекомендовано МО.
15. Таненбаум Э. С. Современные операционные системы / Э. Таненбаум. - СПб., 2007. - 1037 с. : ил.
16. Таненбаум Э. С. Операционные системы. Разработка и реализация / Э. Таненбаум, А. Вудхалл. - СПб., 2007. - 702 с. : ил. + 1 CD-ROM.
17. Партыка Т. Л. Операционные системы, среды и оболочки : учебное пособие / Т. Л. Партыка, И. И. Попов. - М., 2003. - 399 с. : ил.