Государственный экзамен по специальности (Информатика)

Кафедра Информатики НБИК

Программа для государственного экзамена по специальности

Алгоритмы и протоколы передачи данных

1. Понятие количества информации и информационная энтропия. Алгоритмы модуляции и кодирования при передаче данных, шумы и теорема Шеннона. Источники наводок (NEXT, FEXT) и природа шумов.
2. Алгоритмы сжатия данных. Алгоритм Зива-Лемпеля. Статический алгоритм Хаффмана Сжатие данных с использованием преобразования Барроуза-Вилера
3. Алгоритмы обнаружения и коррекции ошибок. Контроль по четности, CRC.
4. Особенности и методы кодирования голоса. Теорема Найквиста.
5. Алгоритмы работы с изображением. Методы разложения, кодирования и отображения статических и движущихся изображений. Использование несовершенства человеческого зрения при кодировании и отображении. Стандарты MPEG-1 и -2. Интерактивное телевидение.
6. Обзор каналов передачи данных. Кабельные каналы связи. Построение сетей передачи данных с использованием радио каналов. Сопоставление возможностей проводных, радио и оптоволоконных каналов. Источники ограничений.
    - Мобильные телекоммуникации (802.11a-g, WiFi, GSM), спутниковые каналы. Сети Zigbee. Bluetooth. Стандарт широкополосной беспроводной связи IEEE 802.16 (WiMAX). Широкополосный канал для подключения периферийных устройств UWB.
7. Оптоволоконные каналы связи (понятие моды, одно- и мульти-модовые волокна), каналы с открытым лазерным лучом. Оптоволоконные коммутаторы. ламда-switching.
8. Сети передачи данных. Метод доступа.
9. Принципы построения сетевых программных интерфейсов. Алгоритмы и применения сетей P2P
10. Алгоритмы работы с очередями: FIFO, LIFO, LQ, CQ, WFQ, CBWFQ, LLQ. Методы работы в условиях перегрузки. Алгоритмы RED и WRED.
11. Сетевые уровни (7-уровневая модель).
12. Сетевые протоколы уровня L2.
    - Интегрированные сети ISDN. Протокол Frame Relay. Fibre Channel. Синхронные каналы SDH/SONET.
    - Сети управления и сбора данных в реальном масштабе времени (CAN).
13. Сети Ethernet.
    - Повторители, мосты, мультиплексоры, переключатели и маршрутизаторы.
    - Fast Ethernet. GE, 10GE, 40- и 100-гигабитный Ethernet
    - Сети PON, EPON, GEPON.
14. Введение в Интернет. Протокол IPv4 и IPv6, IP-туннели. Протокол UDP.
15. Протокол TCP и его модификации.
16. Протокол передачи команд и сообщений об ошибках (ICMP). Протокол управления перегрузкой для дейтограмм DCCP. Протокол TFRC.
17. Алгоритмы работы с именами и адресами.
    - Протокол DNS (структура, обработка запросов, ресурсные записи).
    - Протокол преобразования адресов ARP
    - Протокол динамического конфигурирования ЭВМ DHCP.
    - Трансляция сетевых адресов (NAT). NetBIOS, WINS.
    - Гипертекстный протокол HTTP. Алгоритмы мультимедиа Протокол управления группами IGMP. Протокол реального времени RTP/RTCP. Протокол резервирования ресурсов RSVP. Протокол запуска сессий SIP.
18. Передача данных с коммутацией по меткам.
    - Качество обслуживания QoS
    - Протокол MPLS, MPLS-TE, GMPLS. Архитектура мультипротокольной коммутации пакетов по меткам.
19. Процедуры Интернет.
    - Удаленный доступ (Telnet/SSH). Протокол пересылки файлов FTP/SCP/TFTP.

- Протокол электронной почты. Многоцелевое расширение почты Интернет (MIME). Почтовый протокол POP3. Протокол Интернет для работы с сообщениями IMAP.
- Современные поисковые системы.
- Сетевой протокол времени NTP.
- Сетевая диагностика. Протокол SNMP. Управляющая база данных MIB.
- Сетевая безопасность. Классификация угроз. Типы атак. IDS, IPS, средства противодействия.

UNIX

1. Оболочка Bourne Shell.
2. Порядок выполнения и процессы.
3. Транспортеры (pipeline).
4. Список команд (command list).
5. Исполнение командной строки.
6. Переменные.
7. Переназначение стандартного ввода/вывода.
8. Операторы.
9. Встроенные команды.
10. Особенности.
11. Фоновые задания.
12. Массивы.
13. Командные файлы: создание, исполнение, комментарий #!.
14. Файл .profile.
15. Справочная система UNIX.
    - Стандартные утилиты. Управление заданиями. Вычислительно-вспомогательные команды
16. Работа с большим количеством файлов (find, split, xargs и т.п.)
17. Печать файлов. Печать в BSD (lpr/lpd). Печать в System V (ATT)
18. X/Window
    - Базовые понятия сетевой графической среды
    - Способы среды запуска (startx и xdm).
    - Window manager. Ресурсы
    - Стандартные параметры графических программ.
    - Xterm. Настройка графической среды.
19. Запуск и остановка системы
    - Запуск системы. rc и inittab
    - Остановка и перезагрузка системы
20. Демоны
    - Назначение демонов. Постоянные демоны
    - Запуск демона посредством супер-демона inetd
    - Особенности взаимодействия с демонами (настройки, сигналы).
21. Управление пользователями
    - Заведение новых пользователей
    - Файл(ы) паролей
    - Типы пользователей
    - Добавление пользователя
    - Удаление пользователя
    - Управление средствами входа. Безопасность системы
    - Отладочные и информационные входы
22. Файловая система

Сетевое программирование

1. Базовые возможности протокола PPP сравнение с протоколом SLIP/CSLIP.
2. Базовый формат кадра PPP. Расширения PPP LCP.
3. Контроль качества линии - PPP LQM.
4. Авторизация в протоколе PPP (протоколы PAP,CHAP,EAP).
5. Особенности инкапсуляции IP в PPP.
6. Сжатие данных в протоколе CCP PPP
7. Криптование данных в протоколе ECP PPP
8. Расширение ML PPP. Расширение MCML/RTF PPP)
9. Общие принципы построения сетевых контрольных протоколов PPP
10. Инкапсуляция PPP в других протоколах. Функции IP DS ()

11. IP unicast, anycast, broadcast, multycast, функции IGMP. Мобильное IP
12. Инкапсуляция IPIP. Протокол IPComp. Понятие об IPSec
13. Инкапсуляция IP в других протоколах, использование ARP,UNARP,InARP
14. Базовые возможности IPv6 Базовые функции ICMPv6 и MLD
15. Функции ND в ICMPv6
16. Тунелирование и совместное использование IPv4 и IPv6
17. Типы сокетов, адресное и протокольное семейства, основные заголовочные файлы и типы данных
18. Активный и пассивный сокет, установление соединения, передача/прием данных
19. Представление данных XDR и языки описания XDR и RPC
20. Принципы построения RPC, его структура и транспорт
21. Способы аутентификации, контроля целостности и защиты данных в RPC
22. Базовые функции и особенности протоколов NFS

Маршрутизация

1. Маршруты и маршрутная таблица. Атрибуты маршрута; организация маршрутной таблицы; методы поиска в маршрутной таблице (бинарные деревья, поиск по байтовым границам, деревья PATRICIA).
2. Статическая маршрутизация. Маршрут «по умолчанию», плавающие и альтернативные маршруты, балансировка нагрузки при статической маршрутизации.
3. Динамическая маршрутизация.
4. Алгоритмы Дикстра и Белмана-Форда для поиска наилучших путей в графах. Формальное описание алгоритмов; вычислительная производительность алгоритмов.
5. Протокол RIP. Работа протокола; проблемы и ограничения RIP.
6. Протокол OSPF:
    - Особенности OSPF, метрика OSPF, формальный граф сети OSPF.
    - Функции протокола. База LSA; распространение маршрутной информации; hello, flooding, synchronization;
7. Технологии «быстрой маршрутизации» (switching technologies). Понятие маршрутного «кеша»; cisco fast switching; cisco netflow switching.
8. Основные понятия междоменной маршрутизации. Автономная система; протокол междоменной маршрутизации; политика маршрутизации; база данных маршрутной политики.
9. Протокол BGP:
    - Сообщения BGP. Open, update, keepalive, notification; машина конечных состояний.
    - Атрибуты маршрута и управление трафиком.
    - Управление крупномасштабными системами и вопросы стабильности. Необходимость полной связанности IBGP; отражатель маршрутов; конфедерации; мягкая переконфигурация и разгрузка маршрутов.
10. Понятие групповой маршрутизации; групповые адреса канального и сетевого уровней; режимы dance-mode и sparse-mode; алгоритмы fooding, RPB, RPM.

Информационная и сетевая безопасность

1. Понятие о защите информации от природных и преднамеренных воздействий. Принципы помехоустойчивого кодирования для защиты от случайных и преднамеренных воздействий.
2. Линейные коды, исправляющие ошибки: построение и основные свойства. Смежные классы линейных кодов.
3. Основные идеи декодирования: синдромное декодирование, декодирование по максимуму правдоподобия, декодирование в ограниченном шаре.
4. Порождающая и проверочная матрицы систематического линейного кода. Циклические коды, исправляющие ошибки: построение и основные свойства (Код Хемминга, коды БЧХ).
5. Конечные поля Галуа. Коды Рида-Соломона. Декодирование кодов Рида-Соломона.
6. Итеративные и каскадные конструкции кодов, идея итеративного декодирования.
7. Многомерные кодовые конструкции для защиты от преднамеренных помех.
8. Оценка вероятности отказа и ошибочного декодирования.
9. Псевдослучайные последовательности. Регистры с обратной связью. Комбинирование нескольких регистров с обратной связью: период и эквивалентная линейная сложность.
10. Защита линий связи от несанкционированного чтения информации. Методы определения кодовой конструкции и скремблера по наблюдениям в линии связи.
11. Задачи шифрования информации. Классические шифры: шифр Цезаря, шифр Вернама, одноразовый блокнот, матричные преобразования как шифры.

12. Частотная атака Касиски. Избыточность источника сообщений и расстояние единственности. Определение совершенной криптосистемы.
13. Стандарт шифрования DES – описание и применение, преобразование ключей.
14. Односторонние функции. Система Диффи-Хелмана распределения секретных ключей. Элементы теории конечного поля.
15. Концепция секретной системы с открытым ключем. Система RSA – описание, свойства и основные атаки.
16. Система Эль Гамаля – описание, свойства и основные атаки.
17. Система МакЭлиса – описание, свойства и основные атаки.
18. Генерация простых чисел. Критерии простоты чисел.
19. Быстрая факторизация целых чисел. Быстрое вычисление дискретного логарифма.
20. Цифровая подпись и хеш-функции.
21. Аутентификация, сертификация, проблемы распределения ключей.

Рекомендуемая литература

1. Семенов Ю.А. “Протоколы Интернет. Энциклопедия”, “Горячая линия. Телеком. М.2001.
2. Семенов Ю.А. “Алгоритмы телекоммуникационных сетей”, том 1. “Алгоритмы и протоколы каналов и сетей передачи данных”, Бином, Москва 2007. (Интернет-Университет Информационных технологий).
3. http://book.itep.ru.
4. С.Баурн. Операционная система UNIX, Москва, изд. МИР, 1986.
5. Б.В.Керниган,Р.Пайк. UNIX - универсальная среда программирования. Москва, изд. «Финансы и статистика», 1992.
6. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М. «Мир» 1986.
7. Габидулин Э.М., Афанасьев В.Б. Кодирование в радиоэлектронике. М. «Радио и связь» 1986.
8. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2001.
9. Чмора А.Л. Современная прикладная криптография: Учебное пособие. – М.: Гелиос АРВ, 2001.

Примеры вопросов на государственном экзамене

Четвертым вопросом всегда является магистерская работа студента (краткое описание, состояние на текущий момент). Выдается для подготовки два варианта билета. Какой из них нужно отвечать, определяется непосредственно на экзамене. Для подготовки к ответу могут быть предложены и другие вопросы из программы, отсутствующие в данном перечне.

Вариант 1

1. Особенности моделей реализации протокола TCP
2. Операторы цикла shell
3. Авторизация в протоколе PPP . Протоколы PAP, CHAP, EAP.

Вариант 2

1. Принципы, на которых базируются алгоритмы коррекции ошибок.
2. Чем определяются права доступа к файлам и другим ресурсам системы.
3. Особенности прав суперпользователя.

Вариант 3

1. Функции IP DS (RFC-2474, -2475, -2481) Особенности работы прокси-серверов
2. Дисковые квоты, установка и измерение
3. Особенности инкапсуляции IP в PPP

Вариант 4

1. MPLS-TE (принципы реализации)
2. Сигналы Unix. Способы отправки, права. Способы приема (обработки) в C и в Shell
3. Особенности протокола PPP сравнение с SLIP/CSLIP

Вариант 5

1. Особенности маршрутизации для мультимедиа
2. Загрузка системы UNIX в однопользовательском режиме. Назначение однопользовательского режима.
3. Расширение MultiLink PPP

Вариант 7

1. Маршрутизация дл MPLS

2. Выполнение заданий по времени. Периодические задания. Выполнение задания в указанное время
3. Общие принципы построения сетевых управляющих протоколов PPP на примере RFC-1377, -1378, -1552, -1638, -1762-64, -1841, -1963, -2043, -2097

Вариант 8

1. Алгоритмы, используемые для сжатия данных
2. Процедура запуска новых процессов в UNIX
3. Шифрование данных в протоколе ECP PPP (RFC-1915, -1968, -2419, -2420)

Вариант 9

1. Особенности алгоритмов маршрутизации. Метрики.
2. Переменные shell, используемые им самим
3. Сжатие данных в протоколе CCP PPP (RFC-1962, -1967, -1974-79, -1993)

Вариант 10

1. Техника реализации QoS в локальных сетях
2. Особенности использования socket в UNIX и в Интернет
3. Контроль качества в PPP LQM

Вариант 11

1. Виртуальные локальные сети и алгоритм STP
2. Файловые системы в UNIX
3. Расширение MCML PPP

Вариант 12

1. Особенности кодового мультиплексирования (отличие от частотного)
2. Обработка параметров командных файлов shell
3. Протокол PPP IPCP

Вариант 13

1. ламбда-коммутация в оптических каналах
2. Организация входа пользователя в систему
3. Протокол PPP LCP

Вариант 14

1. Сетевая безопасность и протокол HTTP
2. Средства безопасности UNIX
3. Блокирующие и не блокирующие socket’ы

Вариант 15

1. Наиболее опасные сетевые атаки
2. Командная строка shell. Порядок разбора и выполнения.
3. Инкапсуляция PPP на примере RFC-1598, -1618-19, -1973, -2363-64, -2516.

Вариант 16

1. DDoS-атаки
2. Переменные shell. Область действия, подстановка значений.
3. Сопоставление IPv4 и IPv6

Вариант 17

1. Особенности протоколов маршрутизации, базирующихся на векторе расстояния
2. Способы обмена данными между процессами в UNIX
3. Назначение протокола ICMP

Вариант 18

1. Методы противодействия SPAM
2. Атрибуты процесса
3. Маршутизация с метрикой состояния канала

Вариант 19

1. Особенности каналов на основе одно- и мультимодовых волокон
2. Процессы зомби
3. Что такое политика маршрутизации?

Вариант 20

1. Методы сетевой диагностики
2. Блочные алгоритмы шифрования
3. Управление заданиями в UNIX

Вариант 21

1. Алгоритмы опорных сетей

2. Электронная подпись
3. Базовые принципы сетевой безопасности

Вариант 22

1. Мобильные телекоммуникации
2. Двухключевые алгоритмы шифрования
3. Общие принципы построения сетевых контрольных протоколов (LCP/NCP)

Вариант 23

1. Принцип оптимальности в маршрутизации
2. Средства обеспечения сетевой безопасности (Firewall, IDS, IPS, Honeypot)
3. Файловая система UNIX

Вариант 24

1. Особенности моделей реализации протокола TCP
2. Операторы цикла shell
3. Авторизация в протоколе PPP . Протоколы PAP, CHAP, EAP.

Вариант 25

1. Принципы, на которых базируются алгоритмы коррекции ошибок.
2. Чем определяются права доступа к файлам и другим ресурсам системы. Особенности прав суперпользователя.
3. Функции IP DS (RFC-2474, -2475, -2481)

Вариант 26

1. Особенности работы прокси-серверов
2. Дисковые квоты, установка и измерение
3. Особенности инкапсуляции IP в PPP

Вариант 27

1. MPLS-TE (принципы реализации)
2. Сигналы Unix. Способы отправки, права. Способы приема (обработки) в C и в Shell
3. Особенности протокола PPP сравнение с SLIP/CSLIP

Вариант 28

1. Особенности маршрутизации для мультимедиа
2. Загрузка системы UNIX в однопользовательском режиме. Назначение однопользовательского режима.
3. Расширение MultiLink PPP

Вариант 29

1. Маршрутизация для MPLS
2. Выполнение заданий по времени. Периодические задания. Выполнение задания в указанное время
3. Общие принципы построения сетевых управляющих протоколов PPP на примере RFC-1377, -1378, -1552, -1638, -1762-64, -1841, -1963, -2043, -2097.

Вариант 30

1. Особенности сетей PON
2. Особенности использования socket в UNIX и в Интернет
3. Контроль качества в PPP LQM

Вариант 31

1. Виртуальные локальные сети и алгоритм STP
2. Файловые системы в UNIX
3. Расширение MCML PPP

Вариант 32

1. Особенности кодового мультиплексирования (отличие от частотного)
2. Обработка параметров командных файлов shell
3. Протокол PPP IPCP

Вариант 33

1. Виртуальная сеть VPLS
2. Организация входа пользователя в систему
3. Протокол PPP LCP

Вариант 34

1. Сетевая безопасность и протокол HTTP
2. Средства безопасности UNIX
3. Блокирующие и не блокирующие socket’ы

Вариант 35

1. Наиболее опасные сетевые атаки
2. Командная строка shell. Порядок разбора и выполнения.
3. Инкапсуляция PPP на примере RFC-1598, -1618-19, -1973, -2363-64, -2516.

Вариант 36

1. DDoS-атаки
2. Переменные shell. Область действия, подстановка значений.
3. Сопоставление IPv4 и IPv6

Вариант 37

1. Особенности протоколов маршрутизации, базирующихся на векторе расстояния
2. Способы обмена данными между процессами в UNIX
3. Назначение протокола ICMP

Вариант 38

1. Методы противодействия SPAM
2. Атрибуты процесса
3. Маршутизация с метрикой состояния канала

Вариант 39

1. Особенности каналов на основе одно- и мультимодовых волокон
2. Процессы зомби
3. Что такое политика маршрутизации?

Вариант 40

1. Методы сетевой диагностики
2. Блочные алгоритмы шифрования
3. Управление заданиями в UNIX

Вариант 41

1. Алгоритмы опорных сетей
2. Электронная подпись
3. Базовые принципы сетевой безопасности

Вариант 42

1. Мобильные телекоммуникации
2. Двухключевые алгоритмы шифрования
3. Общие принципы построения сетевых контрольных протоколов (LCP/NCP)

Вариант 43

1. Принцип оптимальности в маршрутизации
2. Средства обеспечения сетевой безопасности (Firewall, IDS, IPS, Honeypot)
3. Файловая система UNIX

Вариант 44

1. Сравнение технологии обмена данными в системе master-slave и в P2P
2. Краткий обзор различных классов сетевых атак
3. Сравнение систем коррекции ошибок в алгоритмах Хэмминга и Рида-Соломона

Вариант 45

1. Различные алгоритмы работы с очередями в сетевых устройствах
2. Система распределения секретных ключей Диффи-Хелмана
3. Методы оптимизации работы баз данных

Вариант 46

1. Протокол для опорных сетей IEEE 802.17
2. Особенности алгоритма Эль-Гамаля
3. Обоснование использования SQL

Вариант 47

1. Базовые принципы работы протоколов IPSec
2. Алгоритм Беллмана-Форда
3. Особенности использования thread’ов в UNIX

Вариант 48

1. Особенности протокола BlueTooth
2. Программное обеспечение, применяемое для управления VIP ресурсами. Используемые языки программирования, основные функции, достоинства и недостатки существующих решений.
3. Алгоритм выбора маршрута Дикстры

Вариант 49

1. Методы обеспечения качества обслуживания в локальных сетях
2. Программное обеспечение, применяемое для управления VIP ресурсами. Используемые языки программирования, основные функции, достоинства и недостатки существующих решений
3. Канал для подключения периферийных устройств UWB

Вариант 50

1. Протокол GMPLS
2. Защита БД от несанкционированного доступа. Назначение прав доступа к данным (на примере Oracle)
3. Сопоставление протоколов DCCP (Datagram Congestion Control Protocol) и TFRC (TCP Friendly Rate Control)

Вариант 51

1. Мобильные коммуникации WiFi
2. Защита БД от несанкционированного доступа. Назначение прав доступа к данным (на примере Oracle)
3. Методы сетевой диагностики

Вариант 52

1. Протокол MPLS, причины сокращения RTT при его использовании
2. Управление ресурсами в ОС
3. Основные составные части интерпретатора

Вариант 53

1. Протокол L2TP
2. Уязвимости протокола SSL
3. Различные модели реализации протокола TCP

Вариант 54

1. Преимущества объектно-ориентированных языков (откуда они берутся)
2. Алгоритмы семейства MPEG
3. Протокол HTTP

Вариант 55

1. Сопоставление принципов IntServ и DiffServ
2. Почтовые протоколы
3. VPN

Вариант 56

1. Системы Firewall, IPS, IDS, Honeypot
2. Алгоритмы FEC
3. Способы выявления SPAM

Вариант 57

1. Маршрутизация для мультимедиа
2. Выполнение заданий по времени. Периодические задания. Выполнение задания в указанное время
3. Общие принципы построения сетевых управляющих протоколов PPP на примере RFC-1377, -1378, -1552, -1638, -1762-64, -1841, -1963, -2043, -2097.

Вариант 58.

1. Принципы, на которых базируются алгоритмы сжатия данных.
2. Процедура запуска новых процессов в UNIX
3. Методы противодействия SPAM

Вариант 59

1. Основные принципа протоколов IPSec
2. Выполнение заданий по времени. Периодические задания. Выполнение задания в указанное время
3. Шифрование данных в протоколе ECP PPP (RFC-1915, -1968, -2419, -2420)

Вариант 60

1. Различные алгоритмы работы с очередями в сетевых устройствах
2. Дисковые квоты, установка и измерение
3. Общие принципы построения сетевых управляющих протоколов PPP на примере RFC-1377, -1378, -1552, -1638, -1762-64, -1841, -1963, -2043, -2097Б.