**«Утверждаю»**
Председатель методической
комиссии ф-та ПМ-ПУ
_____ А.Ю.Утешев
«___» _____ 2008 года

# ТЕМАТИЧЕСКИЙ ПЛАН

Курса лекций и практических занятий по направлению

**Информационные технологии программирования**

***«Архитектура и безопасность Windows сетей» (72 ак. часа)***

**Лектор – ст.преп. С.Ю.Севрюков**

Построение локальной сети на основе Windows платформ.

1. Принципы построения малых и больших локальных сетей. Клиент-серверная архитектура.
2. Понятие протокола обмена данными. Стек протоколов TCP/IP. Модель OSI (Open Systems Interconnection).
3. Принципы сетевого взаимодействия, аппаратное обеспечение. Классификация сетевых устройств.
4. Архитектура локальной сети на основе Windows платформ. Проектирование и разработка внутренних стандартов при построении локальной сети.
5. Установка серверной ОС MS Windows. Особенности установки клиентской ОС MS Windows.
6. Понятие доменной структуры. Принципы построения доменной структуры.
7. Инструментарий администрирования MS Windows . Консоли управления и оснастки.
8. Формирование адресного пространства сети. DNS, DHCP, выбор и настройка протоколов.
9. Конфигурирование сетевой привязки клиентских машин в рамках доменной структуры.
10. Служба каталога Active Directory. Основные понятия и элементы AD.
11. Конфигурирование AD.
12. Другие службы MS Windows. Основные характеристики и назначение.

Обеспечение безопасности в MS Windows .

1. Общие понятия безопасности. Процесс обеспечения безопасности. Обобщённый алгоритм построения защищённой системы.
2. Категории обеспечения безопасности. Ключевые этапы построения защищённой системы.
3. Категории нарушения безопасности. Разработка общей политики безопасности.
4. Общие концепции защиты Windows . Основные компоненты защищённости. Области безопасности.

5. Модель управления доступом в Windows . Типы защищаемых объектов.
6. Маркер доступа. Информация доступная в маркере доступа.
7. Дескриптор безопасности. DACL и SACL. Набор информации для определения доступа к защищаемому объекту.
8. Идентификатор безопасности. SID и RID.
9. Привилегии и права пользователя. Различия, назначение и область действия.
10. Механизм управления доступом.
11. Инструментарий, используемый для управления безопасностью компьютера и объектов. Стандартные средства управления безопасностью. Дополнительный инструментарий и утилиты сторонних производителей.
12. Инструментарий для управления автономным компьютером.
13. Инструментарий для управления компьютером в составе домена.
14. Active Directory, Users and Computers. Sites and Services.
15. Инструментарий для управления различными областями безопасности.
16. Настройка параметров безопасности через политики. Account Policies. Security Configuration and Analysis. Group Policy Editor. Local Security Policy. File System. System Services. Event Log Settings. Registry. Restricted Groups. Public Key Policies. IP Security Policies.
17. Дополнительные инструменты и программные средства для проверки и анализа безопасности.
18. Понятие политики безопасности. Задачи управления через применения политик.
19. Порядок применения политики. Структура групповой политики.
20. Разделы и шаблоны политики. Виды и особенности шаблонов преопределённые в системе.
21. Управление доступом в Windows и проверка подлинности пользователей.
22. Основные механизмы управления доступом.
23. Служба аутентификации.
24. Протоколы аутентификации.
25. Понятие простой аутентификации. Применение политики паролей. Интерактивный вход в систему.
26. Протокол аутентификации Kerberos. Процесс взаимодействия компонентов в службе Kerberos.
27. Интерактивный вход в систему с использованием службы Kerberos.
28. Настройка протокола Kerberos. Влияние синхронизации времени.
29. Утилиты для администрирования процесса аутентификации.
30. Использование учётных записей пользователей и групп. Рекомендации для политики наименования и создания идентификаторов. Категории учётных записей.
31. Рекомендации по контролю учётных записей пользователей.
32. Использование групп в Windows . Концепция использования групп. Разновидности групп.
33. Стандартные группы и их права в системе.
34. Стратегия управления членством в группах. Стратегия развёртывания групп безопасности.
35. Инструментарий для управления группами.
36. Обеспечение защиты данных на уровне файловой системы и управление доступом. Особенности управления доступом к файловой системе.
37. Списки управления доступом. Утилиты управления доступом.
38. Файловая система с шифрованием EFS. Механизм работы EFS.
39. Утилиты для работы с шифрованием EFS.

40. Наблюдение за параметрами безопасности системы. Аудит.
41. Аудит файлов и каталогов. Аудит реестра. Аудит принтеров. Аудит службы удалённого доступа.
42. Просмотр событий аудита. Рекомендации по использованию журнала событий.
43. Оповещения. Утилиты аудита.
44. Устранение ошибок операционной системы. Управление развёртыванием исправлений в организации.
45. Тестирование и анализ пакетов исправлений. Развёртывание пакетов исправлений.
46. Программные средства контроля неустановленных исправлений.