

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ
КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Ордена Трудового Красного Знамени федеральное государственное бюджетное
образовательное учреждение высшего образования

**МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И
ИНФОРМАТИКИ**

Кафедра Сетевые информационные технологии и сервисы

Учебно-методическое пособие и задание на курсовую работу по дисциплине
«Управление и администрирование информационных систем»
Для направления: 09.03.02

Учебно-методическое пособие и задание на курсовую работу по дисциплине
«Управление и администрирование информационных систем»

Авторы (составители):

Беленькая Марина Наумовна (ст. преподаватель)

Гадасин Денис Вадимович (к.т.н., доцент)

Шведов Андрей Вячеславович (ст. преподаватель)

Издание утверждено советом факультета Информационные
технологии. Протокол № _____ от « _____ » _____ 20__ г.

Рецензент: внутренний (Кальфа Александр Алексеевич, д.ф-м.н., профессор)

1. Общие замечания

1.1. Цели и задачи дисциплины.

Целью преподавания дисциплины УиАИС в системе подготовки по направлениям 09.03.02 является теоретическая и практическая подготовка, которая должна обеспечить получение у студентов углубленных представлений о методах администрирования в информационных системах, способах реализации систем управления информационными системами. В результате изучения дисциплины студенты должны:

Знать – функции и задачи администрирования информационных систем, типы объектов управления в информационных системах, различные модели управления и их назначение, протоколы и стандарты администрирования, особенности администрирования кабельных систем, сетевых систем, операционных систем и СУБД, способы администрирования серверов.

Уметь – использовать средства диагностики неисправностей, конфигурации, учета и аудита в информационных системах, анализировать проблемы безопасности информационных системах и применять средства защиты от несанкционированного доступа, определять проблемы потери производительности в информационных системах и применять способы ее повышения, реализовывать методы архивирования и восстановления, методы сопровождения и эксплуатации информационных систем.

Иметь представление – о способах программирования и проектирования систем администрирования, архитектуре систем администрирования и их видах, принципах работы протоколов SNMP и NetFlow.

Для изучения дисциплины предусмотрены следующие виды учебных занятий: лекции, лабораторные работы, практические занятия, выполнение курсовой работы, самостоятельная работа студентов.

Методические указания отражают содержание разделов программы курса, основные понятия, контрольные вопросы по курсу, задание на выполнение курсовой работы.

1.2. Основные понятия и определения

1.2.1. Администратор системы (системный администратор) – это человек или группа людей, которые создают и затем эксплуатируют информационную систему предприятия. Он или они могут быть сотрудниками служб информационных технологий компании и выполняют широкий набор функций:

- установка и сопровождение компьютерных сетевых и информационных систем;
- определение и согласование с фирмами-поставщиками всей аппаратно-программной и организационной части по реализации системы;
- планирование развития информационных систем и внедрения сервисов;
- решение вопросов ведения проектов;
- обучение технического персонала и пользователей;
- консультирование по компьютерным проблемам персонала предприятия и технических служб;
- решение проблем сбора статистики, мониторинга, диагностики, восстановления и сохранения системы, а также всех вопросов организации, соответствующих программных и аппаратных продуктов для этой деятельности;
- разработка программных продуктов на языках управления заданиями (например, на скриптах) с целью создания технологии работы компании и синхронизации работы компонент информационной системы;
- определение ошибок в работе прикладных, системных и аппаратных средств, используемых предприятием, и решением вопросов по их устранению.

Раньше все эти функции выполнялись отделами системного программирования вычислительных центров предприятий. В настоящее время эти функции, как правило, выполняются совокупностью информационных служб предприятия, а именно:

- службами управления: конфигурацией, контролем характеристик, ошибочными ситуациями, безопасностью, производительностью;
- службами планирования и развития;
- службами эксплуатации и сопровождения;
- службами общего управления.

Профессиональные навыки специалистов, работающих в службах администрирования информационных систем (ИС) должны быть достаточно высоки. Так, с учетом функций по администрированию ИС, системные администраторы должны обладать знаниями в области:

- теории операционных систем (ОС) и практики их установки;
- теории баз данных и вопросов администрации СУБД, вопросов поддержки целостности данных;
- сетевых технологий, сетевого оборудования (конфигурации и применения коммутаторов и маршрутизаторов), вопросов диагностики сетевых проблем;
- электротехники и реализации кабельных систем для целей передачи данных;
- реализации веб-приложений и организации доступа к веб-сайтам;
- защиты информации от несанкционированного доступа, включая администрирование специальных устройств (firewall) и консультации пользователей по вопросам защиты их информации;
- вычислительной техники, начиная с простейших операций и заканчивая архитектурой центров обработки данных (ЦОД);
- основ проектирования информационных систем, прикладного программирования;
- способов восстановления информации и реализации подсистем ввода-вывода,
- файловых подсистем;
- языков программирования;

- методов управления в информационных системах и соответствующих аппаратно-программных комплексов.

Кроме того, администратор системы должен уметь общаться с людьми, объяснять им способы решения проблем и убеждать их в своей правоте.

1.2.2. Область деятельности системных администраторов должна охватывать управление всех компонент информационной системы.

Управление (администрирование) ИС – это совокупность действий, осуществляемых администратором системы средствами самой ИС, обеспечивающих сохранение и/или развитие ее свойств в заданном направлении. В полном объеме управлять всеми компонентами ИС и всеми ее функциональными подсистемами может только непосредственно руководство предприятия. АС обычно выполняет задачи управления обеспечивающих подсистем и частично задачи управления функциональных и организационных подсистем в рамках, переданных ему руководством предприятия полномочий

В настоящее время администрирование ИС чаще всего осуществляется в условиях, когда эти системы являются открытыми и гетерогенными. Корпоративной ИС называется информационная система, виртуально объединяющая (в информационном плане) все части одной организации, которые могут находиться в разных городах, частях страны или земного шара. Доступ пользователей в корпоративную систему возможен только для членов компании, ее клиентов или ее контрагентов. В то же время, множество информационных систем сегодня пересекают национальные, коммерческие и континентальные границы для обеспечения глобального взаимодействия большого числа организаций и физических лиц. Такие ИС называются глобальными. В широком смысле открытой системой может быть названа любая система (компьютер, вычислительная сеть, операционная система, программный продукт), которая построена в соответствии с открытыми спецификациями для интерфейсов, служб и форматов. При этом используются различные интерфейсы и средства передачи данных, различное программное

обеспечение и различная архитектура ЭВМ. То есть практически любая система является разнородной или гетерогенной, включающей в себя оборудование и программное обеспечение нескольких производителей. Особую роль при создании таких систем играют стандарты. Без стандартизации работоспособность таких систем невозможна, поскольку программное обеспечение одного производителя “не поймет” программное обеспечение другого. Стандарт – это вариант реализации протокола в аппаратуре или программном обеспечении, который отражается в документе, согласованном и принятом аккредитованной организацией, разрабатывающей стандарты. Стандарт содержит правила, руководства или характеристики для работ, или их результатов с целью достижения оптимальной степени упорядочения и согласованности в заданном контексте. В табл. 1 приведены основные стандартизирующие организации:

Табл. 1. Международные стандартизирующие организации и их
официальные сайты

Стандартизирующая организация	Официальный сайт
ISO	www.iso.org
ANSI	www.ansi.org
MEF	www.metroethernetforum.org
IETF	www.ietf.org
ITU	www.itu.int
IEC (International Engineering Consortium)	www.iec.org
IEC (International Electrotechnical Commission)	www.iec.ch
IEEE	www.ieee.org
EIA	www.eia.org
TIA	www.tiaonline.org
ECMA	www.ecma-international.org
IAB	www.iab.org

В процессе администрирования ИС администратор системы должен руководствоваться некоей моделью администрирования. Модель

администрирования (управления) в ИС – это набор функций по управлению подсистемой или информационным процессом.

Различные стандартизирующие организации предлагают различный набор функций (различные модели) по управлению техническим обеспечением, организационной и функциональной подсистемами. Это модели ISO-OSI, ISO FCAPS, OGC ITIL, ITU TMN, TMF eTOM. На сегодняшний день модель FCAPS – это основная модель администрирования не только сетевых систем, но и любых ИС, как систем передачи данных. В рекомендациях ITU-T X.700 и в стандарте ISO 7498-4 описаны пять функциональных групп модели FCAPS:

(F) Fault Management (Управление отказами) – обнаружение отказов в устройствах сети, сопоставление аварийной информации от различных устройств, локализация отказов и инициирование корректирующих действий.

(C) Configuration Management (Управление конфигурированием) – возможность отслеживания изменений, конфигурирования, передачи и установки программного обеспечения на всех устройствах сети.

(A) Accounting Management (Управление учетом) – возможность сбора и передачи учетной информации для генерации отчетов об использовании сетевых ресурсов.

(P) Performance Management (Управление производительностью) – непрерывный источник информации для мониторинга показателей работы сети (QoS (Quality of Service, Качество обслуживания), ToS (Terms of Service, Тип обслуживания)) и распределения сетевых ресурсов.

(S) Security Management (Управление безопасностью) – возможность управления доступом к сетевым ресурсам и защитой от угроз.

Далее рассмотрим администрирование подсистем ИС.

1.2.3. Администрирование кабельной системы (КС) предусматривает точное обозначение и учет всех элементов, составляющих кабельную систему, а также кабельных трасс, телекоммуникационных и других помещений, в которых монтируется система, а также контроль состояния КС с целью определения места возникновения проблемы. Возможности передачи данных

ограничены возможностями кабеля. Существует два вида оптического волокна в зависимости от диаметра стеклянного сердечника и стеклянной отражающей оболочки:

- многомодовое волокно – multimode (MM, 62,5/125 мкм и 50/125 мкм);
- одномодовое волокно – singlemode (SM, 9-10/125 мкм).

Световой пучок передается по разным видам оптоволокна на разных длинах волн:

- многомодовое волокно – 850 нм и 1300 нм с затуханием 1,5-5Дб/км;
- одномодовое волокно – 1300 нм и 1550 нм с затуханием 1Дб/км.

В настоящее время широко используются ST-коннекторы и SC-коннекторы. Новое оптическое активное оборудование, разработанное после 1995 года, выпускается только в вариантах с SC-портами. Так как по кабельным системам зданий ведется передача данных, и они подключены к компьютерам, возникли жесткие требования по пожарной безопасности и специальные тесты. Это тесты на соответствие следующим требованиям:

- предотвращение горения (изоляция и оболочка кабельной системы должны быть негорючими);
- отсутствие выделения дыма при пожаре;
- отсутствие токсичных выделений при пожаре (галогенов).

Кабелям, прошедшим этот тест, присваивается маркировка LSZH: L(ow) S(moke) Z(ero) H(alogen). Существуют маркировки для коммуникационных кабелей, частично прошедших тесты (например, CMR или OFNR). Приведем основные стандарты, необходимые для осуществления высокоскоростной передачи данных и обязательные для соблюдения службами администратора системы.

EIA/TIA 568 – стандарт создания телекоммуникаций служебных и производственных зданий, планирование кабельных систем зданий, методика построения системы телекоммуникаций служебных и производственных зданий.

EIA/TIA 569 – стандарт описывает требования к помещениям, в которых устанавливается структурированная кабельная система и оборудование связи. EIA/TIA 606 – стандарт администрирования телекоммуникационной инфраструктуры в служебных и производственных зданиях.

EIA/TIA 607 – стандарт описывает требования к инфраструктуре телекоммуникационной системы заземления и выравнивания потенциалов в служебных и производственных зданиях.

При подключении компьютеров, чаще всего возникает необходимость использовать патчкорды и разъемы RJ-45 для UTP. Во всем новом сетевом оборудовании используется стандарт TIA-568A, о чем следует помнить администратору системы.

В процессе администрирования, все изменения, вносимые в кабельную систему, подлежат документированию. Документирование осуществляется по стандарту ANSI/EIA/TIA-606 (Стандарт администрирования телекоммуникационных инфраструктур коммерческих зданий). АС необходимо подробное изучение данного стандарта

1.2.4. После решения проблемы объединения отдельных компьютеров в сети возникла необходимость соединять сети компьютеров между собой. Это соединение сегментов сетей осуществляется при помощи коммутаторов, маршрутизаторов и других специальных устройств. Сегмент сети – это часть сети, которая не содержит соединяющих устройств. Устройства, соединяющие сегменты одной большой сети, подразделяются на виды в зависимости от функционального уровня OSI, на котором они работают. Так, на первом уровне (Physical) работают усилители/репитеры/хабы, на втором (Data Link) – мосты/коммутаторы, на третьем (Network) – маршрутизаторы (роутеры), на всех уровнях работают шлюзы. Хаб не производит анализа информации. Он на короткое время запоминает значения сигнала «0» или «1», соответствующим образом их регенерирует, усиливает и отправляет во все присоединенные сегменты сети. Мост-устройство, разделяющее сети на сегменты. Он пересылает информацию (фрейм) не всем устройствам сети, а

только в тот сегмент, в котором находится получатель. Мосты работают с физическими адресами станций на канальном уровне протоколов OSI. В отличие от хаба мост может разрешать доступ к физическим устройствам, либо запрещать его, то есть, способен регулировать трафик. Существует три типа протоколов маршрутизации мостов:

TR или STA (transparent, прозрачный или обучающийся) – использует алгоритм STA (Spanning Tree Algorithm), который применяется, например, во всех версиях коммутируемого Ethernet.

SR (source routing, маршрутизация от источника) – информация о маршруте содержится в каждом передаваемом кадре; используется в сети Token Ring IBM.

SRT (source routing transparent) – комбинация двух перечисленных выше типов.

Коммутатор (switch) – это мультипортовый мост. Он обеспечивает передачу фреймов от станции к станции в режиме точка-точка (point to point). При этом станции в сети работают параллельно, то есть передача может вестись одновременно между всеми парами портов. Коммутация осуществляется по физическим адресам устройств (MAC-адресам). При этом при помощи специальных протоколов третьего уровня OSI осуществляется множество функций управления сетевым трафиком.

Существует два типа коммутации:

«Буферная» (store and forward) - фрейм задерживается в буфере до окончания его полной передачи и только после этого транслируется дальше. «Обрезная» или «сквозная» (cut-through) - коммутаторы, использующие этот тип коммутации, называются сквозными, и они начинают транслировать фрейм в выходной порт сразу по получении заголовка, не дожидаясь окончания приема фрейма.

Многие коммутаторы позволяют администраторам задавать дополнительные условия фильтрации фреймов наряду со стандартными условиями их фильтрации в соответствии с информацией адресной таблицы. Для создания дополнительных барьеров на пути фреймов, которые ограничивают доступ

определённых групп пользователей к определённым службам сети, задействуются пользовательские фильтры. Построение сетей на основе коммутаторов позволяет ввести приоритезацию фреймов, причём делать это независимо от технологии сети. Поддержка приоритетной обработки особенно необходима и должна быть использована администратором системы для приложений, предъявляющих различные требования к допустимым задержкам фреймов и к пропускной способности сети, например, IP-телефония, видео. Для всех TR-коммутаторов обязательна поддержка алгоритма покрывающего дерева Spanning Tree (STA). Алгоритм покрывающего дерева предназначен для связи сегментов сетей. Все коммутаторы поддерживают средства организации виртуальных сетей. Виртуальной сетью (VLAN) называется группа станций сети, пакеты которой, в том числе и широковещательные, на канальном уровне полностью изолированы от других станций сети. Объединение станций в такие группы выполняется либо на основе принадлежности к портам коммутатора, либо на основе принадлежности фреймов к одному сетевому протоколу, либо по MAC-адресам станций. При параметризации операционной системы коммутатора тип такого объединения задается администратором системы. Назначение технологии виртуальных сетей состоит в защите от несанкционированного доступа и в создании изолированных сетей, которые затем могут быть связаны с помощью маршрутизаторов, реализующих какой-либо протокол сетевого уровня, например, IP. Для объединения виртуальных сетей в общую сеть требуется использование протоколов сетевого уровня. Они могут быть реализованы в специальном устройстве – маршрутизаторе, а могут работать и в составе программного обеспечения коммутатора, который в этом случае становится комбинированным устройством – так называемым коммутатором 3-го уровня. Администратор системы должен учесть, что выполнение дополнительных функций может снизить производительность коммутатора, так как обработка таблиц, фильтрация и приоритезация трафика, обработка маршрутов требует проведения дополнительных вычислений процессорами портов.

Шлюз (Gateway) – это устройство для соединения подсетей по протоколам выше 3-го уровня OSI. Шлюзы применяются в сложных гетерогенных сетях. Например, если возникает необходимость присоединить сегмент с персональными компьютерами, представляющими символы в коде ASCII, к мейнфрейм, представляющей символы в коде EBCDIC. Тщательное проектирование сети является важнейшей задачей служб администратора системы. Для решения задачи проектирования сетей принят трёхуровневый подход. В этой трёхуровневой модели все сетевые устройства и соединения между ними группируются и подразделяются на три уровня: базовый (магистральный) уровень; уровень распределения; уровень доступа. На каждом уровне требуется свой тип коммутатора, который наилучшим образом решает задачи данного уровня. Функции и технические характеристики каждого коммутатора зависят от уровня, для которого предназначен этот коммутатор.

Маршрутизатор (router) – устройство, работающее на третьем, сетевом уровне модели OSI. Маршрутизатор принимает решения о пересылке пакетов сетевого уровня модели OSI их получателю на основании таблицы маршрутизации и определённых правил. При этом в пределах сегмента он работает на канальном уровне модели OSI, а между сегментами – на сетевом. На сетевом уровне создаётся логический адрес сети. Этот адрес присваивается операционной системой или администратором системы для идентификации группы компьютеров. Такую группу иначе называют «subnet» (подсеть). Маршрутизация реализуется с помощью одного или нескольких протоколов маршрутизации либо при помощи статически настроенных таблиц маршрутизации. Маршрутизация может осуществляться по разным алгоритмам и быть статической или динамической. Наиболее известные протоколы маршрутизации, которые есть обычно у всех маршрутизаторов это: протокол маршрутной информации (Routing Information Protocol) RIP; открытый протокол предпочтения кратчайшего пути (Open Shortest Path First) OSPF.

RIP является дистанционно-векторным протоколом. OSPF более сложный протокол; относится к протоколам состояния канала и ориентирован на применение в больших гетерогенных сетях. Маршрутизаторы выполняют не только функцию маршрутизации, но и функцию коммутации. То есть обеспечивают перенаправление пакетов с входного интерфейса маршрутизатора на выходной интерфейс в зависимости от таблицы маршрутизации. Маршрутизатор производит переупаковку полезной информации из поступающих к нему пакетов различных протоколов второго уровня. Например, из Ethernet в PPP или Frame Relay. Поддержка таблиц маршрутизации осуществляется либо администратором сети вручную, либо с помощью динамических протоколов маршрутизации. В общем случае при построении таблицы маршрутизации маршрутизатор применяет комбинацию следующих методов маршрутизации: прямое соединение; статическая маршрутизация; маршрутизация по умолчанию; динамическая маршрутизация.

1.2.5. Под конфигурацией ИС будем понимать разработку и реализацию концепции, позволяющей администратору системы быть уверенным в непротиворечивости, целостности, проверяемости и повторяемости параметров системы. Можно выделить ряд стандартных проблем и задач конфигурации. К ним относятся следующие задачи: стандартизация параметров, задание параметров при инициализации ресурсов, обеспечение загрузки компонент, восстановление параметров, инвентаризация параметров и документирование функциональных схем работы компонент системы, конфигурация параметров согласно политике организации. Администратору системы необходимо создать профайл (список) параметров данной организации, влияющих на защиту от несанкционированного доступа. Для реализации задач по конфигурации параметров в ОС, СУБД, прикладных системах существуют собственные средства. К этим средствам АС должен добавить дополнительные программные продукты, позволяющие выдавать по расписанию отчеты о конфигурациях, архивировать согласно расписанию и

восстанавливать параметры. Помимо этого, необходимо использовать специальные системы защиты от НСД, например, сетевые средства RADIUS (Remote Authentication Dial-In User Service) /TACAS (Terminal Access-Controller Access Control System), позволяющие централизовать сетевую защиту.

1.2.6. Одна из наиболее важных задач АС – защита от угроз ИС. Угрозой является любая ситуация, вызванная преднамеренно или ненамеренно, и которая способна неблагоприятно повлиять на систему. Преднамеренные угрозы всегда осуществляются пользователями системы или прикладными программистами. Непреднамеренная угроза всегда вызывается сбоями питания, сбоями аппаратных или программных средств, неквалифицированными действиями персонала.

К средствам, мероприятиям и нормам обеспечения безопасности процессов переработки информации, которые используются администратором системы, относятся аппаратные и программные средства, организационные мероприятия, законодательные и морально-этические нормы. Аппаратные средства реализуются в виде электронных или электрических устройств. Они могут быть встроены непосредственно в вычислительную технику или реализовываться автономно, например, электронные замки на дверях помещений. Программные средства выполняют функции защиты процессов обработки информации (например, сетевые экраны – фаерволлы). Обычно все программные продукты включают средства AAA (Авторизация пользователей, Аутентификация пользователей и Аудит системы). Организационные мероприятия представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые администратором системы в процессе установки или эксплуатации ИС. Организационные мероприятия являются наиболее действенными и существенными средствами. Они включают ограничение доступа к частям объекта, где работает ИС, разграничение доступа к ресурсам, разработку документации и инструкций пользователям, сертификацию средств защиты,

контроль выполнения правил. Законодательные нормы определяются законодательными актами страны, регламентирующими правила пользования и обработки информации и устанавливающими меры ответственности за нарушение этих правил.

1.2.7. В зависимости от вида приложений, производительность ИС может определяться различными параметрами: временем отклика приложения, общим временем работы или временем ввода/вывода (total time, I/O time, system time, CPU time). Выделяют четыре этапа по управлению производительностью:

- определение базовой (номинальной) производительности ИС;
- контроль отклонений от нее;
- создание отчетов о производительности;
- коррекция производительности ИС.

Для правильной оценки производительности ИС необходимы параметры - метрики. В качестве метрик должна выступать система параметров количественной и качественной оценки процесса. Предполагается, что метрике соответствует необходимая для проведения измерения процедура и процедура для интерпретации результатов. Так для сетевой подсистемы ИС существует пять ключевых метрик. Две метрики характеризуют передачу информации от источника к принимающему устройству. Это пропускная способность канала и задержка передачи данных (latency, латенция). Три метрики характеризуют состояние устройств – ошибки интерфейсов, утилизация ресурсов сетевых устройств, использование буферов сетевых устройств и файл-серверов. Для файл-сервера, помимо перечисленных выше параметров, влияющих на производительность, важны следующие параметры:

- утилизация процессора;
- параметры работы дисковой подсистемы ввода/вывода;
- параметры ввода/вывода шины процессора;
- параметры ввода/вывода сетевых адаптеров.

Измерение технических метрик не дает в таких сложных системах однозначной оценки производительности или анализа причин ее уменьшения. Поэтому пользуются интегральными характеристиками производительности, которые определяются успешной производственной деятельностью предприятия. Например, время отклика приложения. Администратор системы должен заняться проблемой повышения производительности системы не в любом случае изменения технических метрик, а именно тогда, когда изменилась бизнес-метрика. Эти условия оговариваются в специальном договоре: договоре об уровне обслуживания – SLA (Service Level Agreements). В этом договоре содержатся критерии, согласно которым пользователь ожидает получить оговоренные услуги. Создание договора свидетельствует о том, что службы администратора системы и бизнес договорились о стандарте на производительность системы и способах ее оценки. Согласно этому договору производится сопоставление обещанного уровня качества и того, что есть в реальности. В договоре SLA определяются род предоставляемой услуги, сроки, местоположение, затраты, обязанности вовлеченных сторон. Для измерения параметров, например, сетевых подсистем ИС используются специальные диагностические средства: генераторы и анализаторы трафика. В некоторых ситуациях единственным способом установить время и причину ухудшения производительности сетевой системы, является эмуляция загрузки при помощи генерации трафика. АС должен иметь такие дополнительные программные продукты.

1.2.8. Для сопровождения ИС необходимы регулярные обязательные для исполнения работы, направленные на поддержание эксплуатационных характеристик ИС – регламентные работы. Регламентные работы бывают двух типов: периодические и календарные. Периодические регламентные работы – это те, для которых задается время до выполнения следующей аналогичной работы. Плановая дата каждой работы графика может зависеть от фактической даты выполнения предыдущих работ. Периодичность может быть задана календарными отрезками времени работы оборудования или ПО.

Календарные регламентные работы, которые выполняются по графику, заданному датами начала работ. График может содержать одну или более работ. Плановая дата каждой работы графика может не зависеть от фактической даты выполнения предыдущих работ.

2. Задание на курсовую работу

Задание на курсовую работу составлено в тридцати одном варианте (табл. 2 и табл. 3). Номер варианта равен порядковому номеру студента в журнале группы.

В организации устанавливается инфокоммуникационная система на требуемое количество пользователей. Она будет включать:

- Серверную подсистему одного из следующих производителей по выбору студента: Аквариус, YADRO. В составе:
 - файл-сервер под управлением ОС Windows Server 2019;
 - сервер базы данных под управлением СУБД MySQL и ОС Linux;
 - сервер печати под управлением ОС Windows Server 2019;
 - сервер электронной почты под управлением ОС Windows Server 2019;
 - сервер приложений под управлением ОС Linux;
- сетевую аппаратуру и математическое обеспечение одного из следующих производителей по выбору студента: Булат, Eltex, QTECH, Huawei, iKuai;
- кабельную систему на основе витой пары категории 6 и оптоволоконного кабеля;
- систему сетевого управления;
- систему обеспечения сетевой информационной безопасности.

Организация находится в кампусе. Подключение к городской магистрали осуществляется в одном из зданий. Рабочие станции находятся под управлением ОС Windows 10. К системе должен быть осуществлен удаленный доступ определенного числа пользователей. Должен быть осуществлен доступ к сети Интернет пользователей системы.

Для оценки правильности конфигурации параметров должен быть разработан контрольный пример, включающий в себя:

1. Формализацию исходных данных (таблицу с распределением сотрудников по функциональным подразделениям организации);
2. Выбор и расчет активного и пассивного сетевого и серверного оборудования;
3. Разработку структурной схемы организации связи;
4. Расчет плана логической адресации (IP-адресации);
5. Внедрение технологии VLAN;
6. Разработку логической схемы адресации;
7. Внедрение подсистемы IP-телефонии;
8. Выбор протокола динамической маршрутизации и разработку схемы маршрутизации;
9. Внедрение технологии виртуализации и виртуализацию серверной подсистемы;
10. Внедрение системы обеспечения информационной безопасности.

При выполнении контрольной работы студентом самостоятельно выбираются и даются ответы на 5 контрольных вопросов из п. 3.

Требования к оформлению работы приведены в п. 5.

Таблица 2. Варианты заданий

№ вариант а	Количество зданий в кампусе	Количество пользователей	Количество удаленных рабочих мест сотрудников
1	2	450	0
2	1	270	20
3	3	550	50
4	1	500	10
5	4	750	50
6	2	400	0
7	2	600	25
8	3	520	0
9	4	800	25
10	1	285	60
11	2	470	0

12	1	300	15
13	3	600	60
14	4	900	0
15	2	400	50
16	1	370	25
17	5	1000	150
18	3	700	30
19	1	420	20
20	2	580	35
21	4	560	0
22	3	900	70
23	1	375	50
24	2	485	85
25	3	770	55
26	2	560	20
27	2	745	5
28	1	500	25
29	3	645	45
30	4	800	50
31	5	2000	150

Таблица 3. Варианты заданий

№ варианта	Задание
1	Разработать техническое задание компании-подрядчику на выполнение работ по установке сетевой операционной системы на файл-сервере.
2	Разработать техническое задание компании-подрядчику на выполнение работ по установке СУБД на сервере базы данных
3	Разработать техническое задание компании-подрядчику на выполнение работ по установке NMS
4	Разработать техническое задание компании-подрядчику на выполнение работ по установке сервера печати
5	Разработать техническое задание компании-подрядчику на выполнение работ по установке сервера электронной почты
6	Разработать техническое задание компании-подрядчику на выполнение работ по установке кабельной системы
7	Разработать техническое задание компании-подрядчику на выполнение работ по установке сетевой системы на базе

	оборудования и программного обеспечения выбранного производителя
8	Разработать техническое задание компании-подрядчику на выполнение работ по установке средств информационной безопасности
9	Разработать техническое задание компании-подрядчику на выполнение работ по установке средств сетевой диагностики и защиты от сбоев
10	Разработать техническое задание компании-подрядчику на выполнение работ по установке средств учета
11	Разработать техническое задание компании-подрядчику на выполнение работ по установке средств конфигурации
12	Разработать техническое задание компании-подрядчику на выполнение работ по установке средств контроля производительности
13	Разработать техническое задание компании-подрядчику на выполнение работ по установке средств удаленного доступа к информационной системе
14	Разработать техническое задание компании-подрядчику на выполнение работ по установке средств подключения к сети Интернет
15	Разработать требования по выполнению международных и российских стандартов в информационной системе
16	Разработать требования к реализации сетевых протоколов в информационной системе
17	Разработать требования к реализации протоколов маршрутизации в информационной системе.
18	Разработать требования к реализации канальных протоколов в информационной системе
19	Разработать требования к реализации протоколов управления в информационной системе
20	Разработать стратегию архивирования информационной системы

21	Разработать стратегию восстановления информационной системы
22	Разработать стратегию поиска ошибок в информационной системе
23	Разработать инструкцию по действиям администратора системы при самых распространенных ошибках ETHERNET.
24	Разработать инструкцию по действиям администратора системы при самых распространенных ошибках TCP/IP
25	Разработать инструкцию по действиям администратора системы при ошибках ввода/вывода дисковой подсистемы файл-сервера
26	Разработать инструкцию по действиям администратора системы при потере производительности сервера базы данных на 20%
27	Разработать инструкцию по действиям администратора системы при потере производительности всей информационной системы на 20%
28	Разработать инструкцию по действиям администратора системы при потере производительности подключения к сети Интернет на 20%
29	Разработать инструкцию по действиям администратора системы при потере производительности удаленных пользователей на 20%
30	Разработать инструкцию по действиям администратора системы при потере производительности сетевой системы на 20%
31	Разработать техническое задание компании-подрядчику на выполнение работ по установке сервера приложений

3. Контрольные вопросы по курсу

1. Перечислите функции администратора системы.
2. Чем занимаются службы эксплуатации и сопровождения информационной системы?
3. Дайте определение информационной системы. Из каких компонент она состоит?
4. Что такое управление ИС?

5. Приведите пример не гетерогенной ИС.
6. Дайте определение открытой системы.
7. Протокол и стандарт – это идентичные понятия или нет?
8. Перечислите стандартизирующие организации в области передачи данных.
9. Что такое модель администрирования?
10. Что является объектом администрирования?
11. Опишите пять функций управления модели ISO FCAPS.
12. Чему посвящены основные книги ITIL?
13. В каких организациях применяется модель eTOM ?
14. Почему все приложения в ИС используют технологию RPC?
15. Каковы основные характеристики витой пары категории 6?
16. Что такое одномодовые кабели и когда они применяются?
17. Какой разъем применяется в современной сетевой аппаратуре для подключения оптоволоконных кабелей?
18. Каким образом администратор системы должен учитывать требования пожарной безопасности при реализации кабельной системы здания?
19. Перечислите основные подсистемы кабельной системы здания.
20. Что определяют стандарты EIA/TIA 568, 569, 606 и 607?
21. Почему администратор системы должен перед инсталляцией системы выяснить наличие MDI-X портов сетевого оборудования?
22. Приведите пример маркировки кабеля или порта патч-панели администратором системы
23. На каком уровне протоколов OSI работает мост?
24. Каковы типы маршрутизации мостов?
25. Требуется ли от администратора системы начальная инициализация SR-мостов?
26. Какое сетевое устройство называется коммутатором?
27. Какие типы коммутации используются в современных коммутаторах?
28. Какие дополнительные возможности фильтрации фреймов предоставляют современные коммутаторы администратору системы?

29. Для чего в современных коммутаторах реализован алгоритм покрывающего дерева? Имеет ли смысл его использовать в одной сети?
30. На каких принципах станции сети объединяются в виртуальные сети? Что для такого объединения должен сделать администратор системы?
31. Каковы функции сетевого шлюза?
32. В чем состоит трехуровневая модель проектирования сети?
33. Каковы функции маршрутизатора в сети?
34. Что такое маршрутизация и по каким алгоритмам она осуществляется?
35. В чем суть протокола RIP?
36. Чем протокол OSPF принципиально отличается от протокола RIP?
37. Приведите пример команды конфигурирования протокола маршрутизации.
38. Перечислите основные подготовительные этапы процесса инсталляции ОС.
39. Что нужно сделать администратору системы для инсталляции ОС файл-сервера?
40. Что такое канал ввода/вывода
41. Перечислите основные интерфейсы дисковых подсистем.
42. Каковы этапы подготовки дисковой подсистемы для установки ОС?
43. Каковы задачи администрирования данных и администрирования БД?
44. Каковы действия по инсталляции СУБД?
45. Зачем АБД задает параметры запуска ядра СУБД?
46. Зачем нужен мониторинг СУБД администратору системы?
47. Какую статистику необходимо собирать АБД по БД в целом? По запросам приложений? По отдельным отношениям БД?
48. Что означает аббревиатура «AAA» в контексте мер защиты от несанкционированного доступа?
49. В чем суть автоматического режима устранения ошибок?
50. В чем заключается проактивная стратегия поиска ошибок?
51. Когда администратором системы применяется пассивная технология работы NMS?

52. Какие средства диагностики ошибок входят обычно в состав операционной системы?
53. Перечислите средства эмуляции системной консоли администратора системы, ставшие промышленным стандартом.
54. Приведите пример основных ошибок адресации протоколов TCP/IP.
55. В каких случаях средства безопасности доступа могут помешать зарегистрированному пользователю получить нужный доступ к сети?
56. В чем суть проблемы колебания маршрута?
57. Какие факторы влияют на производительность сети?
58. Дайте определение процесса конфигурации.
59. В чем суть задачи инвентаризации параметров ИС?
60. Что должна включать политика безопасности с точки зрения конфигурации?
61. Перечислите задачи учета.
62. Какие события можно отнести к непреднамеренным угрозам?
63. Перечислите виды преднамеренных угроз безопасности?
64. Каковы средства и мероприятия по обеспечению безопасности ИС?
65. В чем суть политики безопасности магистрального уровня сетевой системы?
66. Как используется список доступа для реализации политики безопасности уровня распределения?
67. Приведите пример средств защиты сетевой безопасности на уровне доступа.
68. Какие ключевые вопросы безопасности обеспечивает протокол IPSec?
69. Каковы мероприятия администратора системы по реализации VPN сети?
70. Что является метриками производительности?
71. В чем суть бизнес - метрик производительности?
72. Поясните сущность Соглашения об уровне обслуживания SLA?
73. Чем и почему опасно внедрение средств контроля производительности?
74. Для чего предназначен протокол SNMP?
75. Перечислите команды SNMP

- 76.Приведите пример состава системы администрирования ИС и назначения отдельных модулей
- 77.Что такое OSS система?
- 78.Зачем нужны регламентные работы?
- 79.Перечислите основные регламентные работы по кабельным подсистемам
- 80.Что входит в ежедневные регламентные работы по активному оборудованию?
- 81.Приведите пример регламентных работ по поддержке серверов.
- 82.Перечислите основные регламентные работы по поддержке ОС.
- 83.Приведите пример расписания копирования БД предприятия.

4. Рекомендованный список источников

1. Администрирование в Информационных системах. Беленькая, Малиновский, Яковенко. Учебное пособие для студ. высш. уч. заведений. Москва. Горячая линия- Телеком, 2011. Утверждено УМО МГТУ им. Баумана.
2. Базы Данных. Томас Конноли, Каролин Бегг. Москва. Вильямс. 2003.
3. Введение в операционные системы. Д.В. Иртегов. Санкт-Петербург. БХВ-Петербург. 2008. Учебное пособие для студ. высш. учебн. заведений.
4. Основы сетевых технологий и высокоскоростной передачи данных. Часть 1. Учебное пособие для студ. высших учебных заведений. Докучаев, Беленькая, Яковенко. Москва. МТУСИ. 2009
5. Основы сетевых технологий и высокоскоростной передачи данных. Часть 2. Учебное пособие для студентов высших учебных заведений. Докучаев, Беленькая, Яковенко. Москва. МТУСИ. 2011. Утверждено УМО МТУСИ.
6. Волоконная оптика. Теория и практика. Бейли Д., Райт Э. «Кудиц-Образ», Москва, 2006.
7. Информационная безопасность и защита информации. В.П. Мельников, С.А. Клейменов, А.М. Петраков. Москва. Академия. 2006. Учебное пособие для студ. высш. учебн. заведений.
8. Информационные системы. О.Л. Голицина, Н.В. Максимов, И.И. Попов. Москва. Учебное пособие для студ. высш. учебн. Заведений. Форум-Инфра-М. 2007.
9. Компьютерные сети. Принципы, технологии, протоколы. В. Г. Олифер, Н. А. Олифер. Учебник для ВУЗОВ. Сакт-Петербург. Питер, 2006.
10. Компьютерные сети. Протоколы и технологии Интернета. Столлинс В., Санкт-Петербург, БХВ-Петербург, 2005.

- 11.NGOSS: Построение эффективных систем поддержки и эксплуатации сетей для оператора связи. Райли Дж., Москва. Альпина Бизнес Букс, 2007.
- 12.Основы передачи голосовых данных по сетям IP. Москва. Вильямс, 2007.
- 13.Программно-технологический комплекс сопровождения СУБД ДИСОД. Прикладная информатика. Беленькая, Гейлер. Москва. Финансы и статистика. 1989.
- 14.Поиск неисправностей. Поддержка и восстановление. Бигелоу Стивен Дж., Санкт-Петербург, БХВ-Петербург, 2005.
- 15.Полный справочник по Cisco. Москва. Вильямс, 2008.
- 16.Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство. Москва. Вильямс, 2007.
- 17.Программа сетевой подготовки Cisco CCNA 1 и 2. Вспомогательное руководство. Москва. Вильямс, 2007.
- 18.Проектирование структур баз данных. Т.Тиори, Дж. Фрай. Москва. Мир. 1985.
- 19.Расширенная карта процессов деятельности телекоммуникационной компании: Учебное пособие. Самуйлов К.Е., Серебренникова Н.В., Чукарин А.В., Яркина Н.В. Москва. Изд-во РУДН, 2008.

5. Требования к оформлению.

Контрольная работа должна быть аккуратно оформлена. Страницы должны быть пронумерованы. Титульный лист должен содержать название курсовой работы, номер варианта, номер группы, номер студента согласно зачетной ведомости, фамилию и инициалы студента. Курсовая работа выполняется в формате MS Word. Шрифт Times New Roman 12. Интервал 1.5. Слева должны быть оставлены поля 30 мм для замечаний.

Работа должна включать содержание, введение, выполненные варианты заданий, ответы на 5 контрольных вопросов, заключение, список использованных источников. Интернет-источники должны быть приведены в разделе дополнительных источников. Следует использовать только официальные сайты компаний-производителей и стандартизирующих организаций.