**1. По принципам построения и способам получения решения модели** разделяют на ***аналитические*** и ***имитационные***. Аналитические модели позволяют получить явные функциональные зависимости для искомых величин или определить численные решения для конкретных начальных условий и количественные характеристики модели. Однако по мере усложнения объекта моделирования построение аналитической модели превращается в трудноразрешимую проблему. В тоже время широкое распространение получили: имитационные модели, которые рассматриваются как проводимые на ЭВМ эксперименты с математическими моделями, имитирующими поведение реальных объектов.

Когда модель достаточно проста, можно вычислить ее соотношения и параметры и получить **точное *аналитическое* решение**. Если в случае с математической моделью возможно аналитическое решение и его вычисление представляется эффективным, лучше исследовать модель именно таким образом, не прибегая к имитационному моделированию. Однако многие системы чрезвычайно сложны, они практически полностью исключают возможность аналитического решения. В этом случае модель следует изучать с помощью имитационного моделирования, то есть многократного испытания модели с нужными входными данными, чтобы определить их влияние на выходные критерии оценки работы системы.

2.

активности, процессы и события - явля­ются конструктивными элементами, с помощью которых описывается динамическое поведение дискретных систем, и на основе которых стро­ятся языки моделирования этих систем.

**Активности.**Характеристики производительности прямо или кос­венно связаны со скоростью, с которой система выполняет свою рабо­ту, поэтому они содержат время в качестве независимой переменной. Работа совершается путем выполнения активностей. Активность явля­ется наименьшей единицей работы. Активность рассматривается как единый дискретный шаг. С каждой активностью связано время выпол­нения. Активность может соответствовать определенному этапу вы­полнения команды в моделировании на уровне регистровых передач или выполнения целого задания в макроскопическом моделировании вычис­лительной системы. Независимо от содержания представляемой дея­тельности активность является единым динамическим объектом, ука­зывающим на совершение некоторой единицы работы.

**Процессы.**Логически связанный набор активностей образует про­цесс, который можно рассматривать как объект, вмещающий или ини­циирующий эти активности. Некоторый процесс может выступать в роли активности или субпроцесса в процессе более высокого уровня. Подобно активностям, процессы представляют собой единые динами­ческие объекты. Выполнение в вычислительной системе определенной операции с дисками можно рассматривать как процесс, включающий в себя активности установки головки записи-чтения, задержки на враще­ние носителя и передачи данных.

Различие между активностями и процессами условно. Операция, определенная на одном уровне как активность, на другом уровне может рассматриваться как процесс. Каждый процесс инициируется другим про­цессом, называемым инициатором. Инициатор может находиться как вне системы, так и внутри нее.

**События.**Активности инициируются в результате совершения со­бытий. Событие представляет собой мгновенное изменение состояний некоторого объекта системы, который может быть как пассивным, так и активным. Окончание активности является событием, совершение которого может возбудить последующие активности. Такие события управляют следованием активностей внутри процесса и являются ло­кальными или внутренними событиями данного процесса. Инициализа­ция активности не означает немедленного ее выполнения. Начало вы­полнения находится в зависимости от наличия определенных условий, в число которых входит и инициализация данной активности. Инициализа­ция активности является результатом окончания заранее указанных од­ной или нескольких активностей. Можно считать, что активность, вы­полнение которой не может быть начато из-за отсутствия необходимых условий, находится в ожидании совершения событий, приводящих к появлению этих условий. События можно разделить на две категории: события следования, которые управляют инициализацией активностей BHjnrpn данного процесса, и события изменения состояний, которые уп­равляют выполнением активностей, относящихся в общем случае к независимым процессам. С точки зрения динамики система рассмат­ривается как совокупность связанных друг с другом процессов, причем вза­имодействие между ними управляется и координируется совершающими­ся событиями.

**Описание прцесса** Правила, описывающие поведение класса процессов, состоят из указаний активностей, входя­щих в процессы в определенных соотношениях следования, условий, управляющих их выполнением, и воздействий, оказываемых процесса­ми на атрибуты и состояния активных и пассивных объектов системы. Эти правила в совокупности называются описанием процесса

**Организация процесса моделирования.** Система выполнения имитационного процесса во времени включает в себя механизм динамического управления активными объектами модели. Ее сложность варьируется в значительных пределах в зависи­мости от класса реализуемого алгоритма.

3.

Имитационныематематические модели применяются тогда, когда техническая система особенно сложна или когда необходим высокий уровень детализации представления процессов, протекающих в ней.

В имитационных моделях моделируемый алгоритм поведения технической системы приближённо воспроизводит сам процесс-оригинал в смысле его функционирования во времени. При этом имитируются элементарные явления, составляющие процесс, с сохранением их логической структуры и порядка протекания во времени. Таким образом, реализуется на ЭВМ специальный алгоритм, который воспроизводит формализованный процесс поведения технической системы. Этот алгоритм по исходным данным позволяет получить информацию об изменении во времени *t* состояний и откликов модели. В этом алгоритме можно выделить три функциональные части: моделирование элементарных подпроцессов; учёт их взаимодействия и объединение их в единый процесс; обеспечение согласованной работы отдельных подпроцессов при реализации математической модели на ЭВМ. Влияние случайных факторов на течение процесса имитируется с помощью генераторов случайных чисел с заданными вероятностными характеристиками. В ходе имитации постоянно фиксируется статистика о состояниях системы и изменениях откликов. Эта статистика либо должным образом обрабатывается в ходе имитации, либо накапливается и по окончании заданного интервала моделирования *ТМ* обрабатывается статистическими методами.

Построение модели состоит из решения двух ос­новных задач. Первая задача сводится к тому, чтобы описать правила, задающие различные виды процессов, происходящих в системе. Вторая, наиболее трудная задача, заключается в том, чтобы указать значения атрибутов процессов или задать правила генерации этих значений.

4.

По мере усложнения производственных процессов и развития наукоёмких технологий появились проблемы с большой начальной неопределённостью проблемной ситуации. В таких задачах всё большее место стал занимать собственно процесс постановки задачи, возросла роль лица, принимающего решение, роль человека как носителя системы ценностей, критериев принятия решения, целостного восприятия. В ходе решения подобных комплексных проблем широко используются понятия «система», «системный подход», «системный анализ».

Теория систем изучает общие законы функционирования систем, классификации систем и их роль в выборе методов моделирования конкретных объектов.

5.

Существует множество определений понятия системы. Рассмотрим те из них, которые наиболее полно раскрывают существенные свойства данного понятия.

«Система представляет собой определённое множество взаимосвязанных элементов, образующих устойчивое единство и целостность, обладающее интегральными свойствами и закономерностями».

Более полное и содержательное общее определение описывает систему «как набор объектов, имеющих данные свойства, и набор связей между объектами и их свойствами».

«Системой можно назвать только такой комплекс избирательно-вовлеченных компонентов, у которых взаимодействие и взаимоотношение приобретает характер взаимосодействия компонентов на получение фокусированного полезного результата».



6.

Выбор показателей качества определяется теми задачами, для решения которых строится модель. Часто наблюдается тенденция имитировать все, что касается поведения объекта исследования. Однако такой подход неверен. При построении модели следует ориентироваться на решение лишь тех вопросов, которые сформулированы в постановке задачи, а не имитировать реальную систему во всех подробностях. На первом этапе решения задачи важно отделить главное, то, что действительно ведет к достижению сформулированной цели, от второстепенного. Выбор цели моделирования определяет характеристики, которые отражают поведение сложной системы. В дальнейшем вся работа сводится к выявлению и детализации тех аспектов функционирования системы, которые имеют отношение к выбранным показателям

7.

*Определение управляющих переменных.*

Выбрать управляющие переменные объекта моделирования, значит, указать те выходные параметры системы, которые имеют отношение к показателям качества, сформированным на первом этапе содержательного описания системы. Иными словами, необходимо указать те характеристики, через которые реализуются показатели качества.

Поясним данную мысль примером. Пусть необходимо произвести расчет коэффициента готовности системы. Для определения этого показателя необходимо знать сколько времени в каждом модельном эксперименте система находилась в исправном состоянии и сколько в состоянии отказа, простоя и восстановления. Таким образом, в данном конкретном примере в качестве контролируемых характеристик объекта моделирования будет выступать время нахождения системы в каждом из перечисленных состояний.

Следующий пример. Если требуется определить вероятность безотказной работы системы, то необходимо фиксировать состояние, в котором система находилась к концу каждого модельного эксперимента. Исправному состоянию приписывается значение 1, неисправному 0. Вероятность безотказной работы определяется как отношение количества успешных модельных реализаций к общему количеству испытаний. Следовательно, в данном примере контролируемой характеристикой модели системы будет ее состояние в каждом модельном эксперименте.

8.

*Детализация описания режимов функционирования системы*

На данном этапе перерабатывается и дополняется имеющаяся информация для возможного выделения алгоритмов функционирования в каждом из режимов работы системы. Составляются временные диаграммы функционирования системы. Определяются наиболее неясные или сложные моменты функционирования компонентов системы, устанавливается последовательность их действий, выделяются вероятные места возникновения конфликтных ситуаций и описывается принятый порядок их разрешения в системе.

Для задач анализа надежности важно указать, в какие периоды система работает под нагрузкой, когда она находится в нерабочем состоянии. Важно также знать характер и величину нагрузки, потому что от этого зависят процессы старения, протекающие в элементах.

Могут быть ситуации, когда разные элементы функционируют по своей собственной программе. Например, в системах управления и защиты энергоблоков атомных станций ряд элементов выполняют функции слежения за параметрами объекта управления. В случае, когда наблюдаемые параметры превышают допустимые уставки, элементы дают команду на срабатывание органов управления. Органы управления переводят установку в неработоспособное состояние. При этом они испытывают ударные нагрузки, так как стержни управления входят в активную зону под действием силы тяжести, кроме того на них может оказываться принудительное воздействие.

Естественно, что для анализа надежности моменты непосредственного выполнения функций объектами куда важнее, чем моменты нахождения в состоянии простоя или ожидания.

9.

*Составление описания внешней среды*

На этом этапе необходимо провести исследование факторов, оказывающих воздействие на моделируемую систему. В состав модели включаются только значимые факторы, влияние которых необходимо учитывать опять же с точки зрения сформулированной постановки задачи. В случае моделирования отдельных аспектов функционирования системы проводится исследовательская работа, цель которой состоит в определении алгоритмов взаимодействия системы с внешней средой. Иногда возможны модификация или пополнение состава управляющих переменных системы из-за детализации алгоритмов взаимодействия Между системой и внешней средой.

С точки зрения анализа надежности важно указать факторы, которые способствуют деградации материалов. Например, повышенная влажность, высокие температуры, наличие радиационной активности -факторы, снижающие надежность элементов и системы в целом.

Таким образом, на каждом шаге данного этапа перерабатывается и дополняется имеющаяся информация о поведении системы в соответствии с поставленными целями моделирования. Результатом является содержательное описание сложной системы, выполненное в терминах соответствующего языка. Информация, не относящаяся к задаче моделирования, отбрасывается.

После выполнения описанных этапов поставлена лишь одна цель моделирования. Далее необходимо перейти к математической постановке задачи моделирования и собственно построению модели.

Отметим, что общего рецепта построения содержательной модели не существует. Однако можно утверждать, что при решении достаточно широкого круга задач модель системы представляется в виде сетевой структуры. Узлы сети являются моделями элементов системы. Дуги выражают связи между элементами. Сеть изображается в виде графа передачи, который строится на основе матрицы, отражающей действительные связи между элементами. Для построения имитационной модели необходимо задать поведение динамических элементов. Как было отмечено в предыдущем параграфе, для этого выделяются активности, процессы и события, имеющие место при функционировании системы. Эти динамические объекты описываются с помощью соответствующих классов, отражающих их поведение, и заданием на этих классах атрибутов.

10.

**локальных сетей.**Рабочие станции и серверы соединяются с кабелем коммуникационной подсети с помощью сетевых адаптеров. Основные функции сетевых адаптеров: организация соединения между компьютерами с требуемой скоростью передачи данных; конвертирование и кодирование/декодирование; контроль правильности передачи данных; формирование пакета данных.

Основные характеристики ЛВС:

* вид физической среды передачи данных (коаксиальный кабель, витая пара, оптико-волоконный кабель);
* максимальное число абонентов сети;
* топология сети;
* максимальная скорость передачи данных;
* программное обеспечение сети;
* надежность.

**глобальных сетей.**Глобальные сети создаются крупными корпорациями (телекоммуникационными, реже иными для собственных нужд) для обеспечения информационного взаимодействия между компьютерами, находящимися в разных странах, на разных континентах.

Компания, которая обеспечивает нормальное функционирование глобальной сети, называется оператором.

Компания, оказывающая платные услуги абонентам сети называется провайдером.

Глобальные сети – это результат укрупнения телекоммуникационных компаний, объединения их сетей. Это обусловлено необходимостью расширения спектра предоставляемых услуг, стоимость которых зависит от того имеет ли компания собственные каналы связи или арендует их у конкурентов.

В основу функционирования глобальных сетей положен многоуровневый принцип передачи сообщений.

11.

**Сетевая модель OSI** (The **Open Systems Interconnection** model**)** — сетевая модель стека (магазина) сетевых протоколов OSI/ISO. Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии.

### Сеансовый уровень**[править | править код]**

Сеансовый уровень (англ. *session layer*) модели обеспечивает поддержание сеанса связи, позволяя приложениям взаимодействовать между собой длительное время. Уровень управляет созданием/завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений.

Протоколы сеансового уровня: ADSP (AppleTalk Data Stream Protocol), ASP (AppleTalk Session Protocol), H.245 (Call Control Protocol for Multimedia Communication), ISO-SP (OSI Session Layer Protocol (X.225, ISO 8327)), iSNS (Internet Storage Name Service), L2F (Layer 2 Forwarding Protocol), L2TP (Layer 2 Tunneling Protocol), NetBIOS (Network Basic Input Output System), PAP (Password Authentication Protocol), PPTP (Point-to-Point Tunneling Protocol), RPC (Remote Procedure Call Protocol), RTCP (Real-time Transport Control Protocol), SMPP (Short Message Peer-to-Peer), SCP (Session Control Protocol), ZIP (Zone Information Protocol), SDP (Sockets Direct Protocol)…

### Транспортный уровень**[править | править код]**

Транспортный уровень (англ. *transport layer*) модели предназначен для обеспечения надёжной передачи данных от отправителя к получателю. При этом уровень надёжности может варьироваться в широких пределах. Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приёма), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных. Например, UDP ограничивается контролем целостности данных в рамках одной датаграммы и не исключает возможности потери пакета целиком или дублирования пакетов, нарушение порядка получения пакетов данных; TCP обеспечивает надёжную непрерывную передачу данных, исключающую потерю данных или нарушение порядка их поступления или дублирования, может перераспределять данные, разбивая большие порции данных на фрагменты и наоборот, склеивая фрагменты в один пакет.

Протоколы транспортного уровня: ATP (AppleTalk Transaction Protocol), CUDP (Cyclic UDP), DCCP (Datagram Congestion Control Protocol), FCP (Fibre Channel Protocol), IL (IL Protocol), NBF (NetBIOS Frames protocol), NCP (NetWare Core Protocol), SCTP (Stream Control Transmission Protocol), SPX (Sequenced Packet Exchange), SST (Structured Stream Transport), TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

### Сетевой уровень**[править | править код]**

Сетевой уровень (англ. *network layer*) модели предназначен для определения пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и «заторов» в сети.

Протоколы сетевого уровня маршрутизируют данные от источника к получателю. Работающие на этом уровне устройства (маршрутизаторы) условно называют устройствами третьего уровня (по номеру уровня в модели OSI).

Протоколы сетевого уровня: IP/IPv4/IPv6 (Internet Protocol), IPX (Internetwork Packet Exchange, протокол межсетевого обмена), X.25 (частично этот протокол реализован на уровне 2), CLNP (сетевой протокол без организации соединений), IPsec (Internet Protocol Security). Протоколы маршрутизации — RIP (Routing Information Protocol), OSPF (Open Shortest Path First).

### Канальный уровень**[править | править код]**

Канальный уровень (англ. *data link layer*) предназначен для обеспечения взаимодействия сетей на физическом уровне и контроля ошибок, которые могут возникнуть. Полученные с физического уровня данные, представленные в битах, он упаковывает в кадры, проверяет их на целостность и, если нужно, исправляет ошибки (формирует повторный запрос повреждённого кадра) и отправляет на сетевой уровень. Канальный уровень может взаимодействовать с одним или несколькими физическими уровнями, контролируя и управляя этим взаимодействием.

Спецификация IEEE 802 разделяет этот уровень на два подуровня: MAC (англ. *media access control*) регулирует доступ к разделяемой физической среде, LLC (англ. *logical link control*) обеспечивает обслуживание сетевого уровня.

На этом уровне работают коммутаторы, мосты и другие устройства. Эти устройства используют адресацию второго уровня (по номеру уровня в модели OSI).

Протоколы канального уровня: ARCnet, ATM, Controller Area Network (CAN), Econet, IEEE 802.3 (Ethernet), Ethernet Automatic Protection Switching (EAPS), Fiber Distributed Data Interface (FDDI), Frame Relay, High-Level Data Link Control (HDLC), IEEE 802.2 (предоставляет функции LLC для подуровня IEEE 802 MAC), Link Access Procedures, D channel (LAPD), IEEE 802.11 wireless LAN, LocalTalk, Multiprotocol Label Switching (MPLS), Point-to-Point Protocol (PPP), Point-to-Point Protocol over Ethernet (PPPoE), Serial Line Internet Protocol (SLIP, устарел), StarLan, Token ring, Unidirectional Link Detection (UDLD), x.25, ARP.

При разработке стеков протоколов на этом уровне решаются задачи помехоустойчивого кодирования. К таким способам кодирования относится код Хемминга, блочное кодирование, код Рида-Соломона.

В программировании этот уровень представляет драйвер сетевой платы, в операционных системах имеется программный интерфейс взаимодействия канального и сетевого уровней между собой. Это не новый уровень, а просто реализация модели для конкретной ОС. Примеры таких интерфейсов: ODI (англ.), NDIS, UDI.

12.

Под топологией (компоновкой, конфигурацией, структурой) компьютерной сети обычно понимается физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи. Топология определяет требования к оборудованию, тип используемого кабеля, допустимые и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети.

К наиболее распространенным методам доступа относятся: Ethernet, ArcNet и Token Ring, которые реализованы соответственно в стандартах IЕЕЕ802.3, IЕЕЕ802.4 и IЕЕЕ802.5.  Кроме того, для локальных сетей, работающих на оптическом волокне, американским институтом по стандартизации ASNI  был разработан стандарт FDDI, обеспечивающий скорость передачи данных 100 Мбит/с.

В этих стандартах канальный уровень разделяется на два подуровня, которые называются уровнями:

* управление логическим каналом (LCC - Logical Link Control);
* управление доступом к среде (MAC - Media Access Control).

Уровень управления доступом к среде передачи данных (MAC) появился, так как в локальных сетях используется разделяемая среда передачи данных. В современных локальных сетях получили распространение несколько протоколов уровня MAC, реализующих разные алгоритмы доступа к разделяемой среде. Эти протоколы полностью определяют специфику таких технологий локальных сетей, как Ethernet,  Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI.

После того, как доступ к среде получен, ею может воспользоваться более высокий канальный уровень – уровень LCC, организующий передачу логических единиц данных, кадров информации, с различным уровнем качества транспортных услуг.

13.

Архитектура или организация построения сети (в том числе локальной и распределенной — *см. далее*), в которой производится разделение вычислительной нагрузки между включенными в ее состав ЭВМ, выполняющими функции “**клиентов**”, и одной мощной **центральной ЭВМ** — “**сервером**”. В частности, процесс наблюдения за данными отделен от программ, использующих эти данные. Например, сервер может поддерживать центральную базу данных, расположенную на большом компьютере, зарезервированном для этой цели. Клиентом будет обычная программа, расположенная на любой ЭВМ, включенной в сеть, а также сама ЭВМ, которая по мере необходимости запрашивает данные с сервера. **Производительность** при использовании клиент—серверной архитектуры выше обычной, поскольку как клиент, так и сервер делят между собой нагрузку по обработке данных. Другими достоинствами клиент—серверной архитектуры являются: большой объем памяти и ее пригодность для решения разнородных задач, возможности подключения большого количества рабочих станций, включая ПЭВМ и пассивные терминалы (см. ”**Терминал ввода—вывода** ” ), а также установки средств **защиты от** **несанкционированного доступа** (как сети в целом, так и отдельных ее терминалов, баз данных и т. д.)

14.

Сети с коммутацией каналов используются в корпоративных сетях в основном для удаленного доступа многочисленных домашних пользователей и гораздо реже - для соединения локальных сетей.

К глобальным телекоммуникационным системам относятся те аппаратные и программные средства, которые соединяют пользователей независимо от их физического положения на планете. Главная черта глобальных сетей – интеллектуализация, позволяющая легко использовать мощности сети с оптимальной эффективностью, при этом минимизируя затраты на обслуживание оборудования. Среди глобальных сетей выделяется несколько основных видов.

Цифровые сети с интегральными модулями используют непрерывную коммутацию каналов, при этом массивы данных обрабатываются в цифровой форме. Пользователи сети имеют доступ только к некоторым функциям, интерфейс не позволяет самостоятельно изменять технические параметры.

Сети Х25 являются наиболее старыми, надежными и проверенными технологиями передачи информации между неограниченным числом пользователей. Главное отличие таких сетей – наличие устройства для «сборки» отдельных блоков передаваемой информации в «пакеты» для наиболее быстрой передачи.

Асинхронный режим передачи данных - современная технология, используемая для широкополосных сетей, которые основаны на оптоволоконных кабелях.

15.

16.

Для передачи данных с использованием возможностей телекоммуникационных технологий применяется специальное программное обеспечение. Это обеспечение функционирует по определенным протоколам или по механизмам, разработанным с целью упростить и стандартизировать работу всех узлов сети, выстроив ее по единому алгоритму.

Так, для передачи по компьютерным сетям разработан стандарт MIME (ssr-Multipurpose Internet Mail Extensions), переводящий данные в формат понятный почтовому серверу. Общение компьютера пользователя и сервера происходит в виде диалога в режиме Клиент-Сервер, где с каждой стороны его участником является определенная программа.

Отдельные программы используются для работы мессенджеров, которые позволяют обмениваться сообщениями, совершать телефонные звонки с передачей голосовой и видеоинформации. Здесь происходит коммуникация не только компьютер - почтовый сервер, к диалогу подключаются и телефонные станции.

17.

Понятие информационной безопасности определяют как защиту информации и разных видов данных от незаконного изучения, использования, уничтожения. Также информационная безопасность подразумевает защиту информации от действий, приводящих к ее несанкционированному распространению. Воздействия, которым подвергаются плохо защищенные данные, могут быть самыми разными.

**Целостность данных** – понятие, определяющее постоянную структуру и содержание информации, особенно в момент передачи или хранения. Информационная безопасность в этом свойстве реализуется, если сведения в системе сходны с данными в документах по семантическим параметрам.

Данные должны быть **достоверными**, проверенными. Это свойство выражается в подтверждении сведений определенным субъектом. Угроза информационной безопасности появляется, когда юридическая значимость данных не подтверждена. Это означает, что документ, описывающий их свойства, важно официально зарегистрировать.

**Доступ к информации** выражается в возможности ее копировать, обрабатывать и удалять на свое усмотрение. Доступ бывает несанкционированным (незаконным, без разрешения на соответствующее действие) и санкционированным. Санкционированный вариант изучения сведений основан на требованиях к разграничению доступа.

Информационную безопасность корпоративной сети обеспечивают два метода:

1. **Фрагментарный.** Изучает источники возникновения конкретных угроз в определенных условиях.
2. **Комплексный.** Обеспечение информационной безопасности осуществляется посредством создания среды, которая отвечает за защищенную обработку данных.

18.

Информационная безопасность сетей ЭВМ и телекоммуникаций в целом – одна из основ­ных проблем XXI в., так как хищение, сознательное искажение и уничтожение информации могут привести к катастрофическим последствиям вплоть до человеческих жертв.

*Защита информации* – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

Архитектура сети, включающая аппаратное обеспечение, является одним из факторов, влияющих на ее безопасность, т.е. некоторые виды сетей безопаснее других.

Любые дополнительные соединения с другими сегментами или подключение к Интернету порождают новые проблемы. Атаки на локальную сеть через подключение к Интернету для того, чтобы получить доступ к конфиденциальной информации, в последнее время получили широкое распространение, что связано с недостатками встроенной системы зашиты информации в протоколах TCP/IP.

По мере развития ПЭВМ, увеличения их количества и доступности все больший размах приобретает информационное пиратство: несанкционированное копирование программных продуктов и данных, финансовые преступления с применением ЭВМ, компьютерные диверсии (вирусы, «логические бомбы», «черви», «троянские кони» и т.п.). Появление глобальных сетей, особенно сети Интернет, еще в большей степени стимулировало такое пиратство, значительно увеличив количество дос­тупных пирату компьютеров за счет исключения необходимости физического доступа к ним и сделав сам процесс более увлекательным в силу его интерактивности.

Сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать:

– целостность данных (защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных);

– конфиденциальность информации;

– доступность информации для всех авторизованных пользователей. В рамках комплексного рассмотрения вопросов обеспечения безопасности информации различают угрозы безопасности, службы безопасности (СБ) и механизмы реализации функций служб безопасности.

19.

***Шифрование***данных представляет собой разновидность программных средств защиты информации и имеет особое значение на практике как единственная надежная защита информации, передаваемой по протяженным последовательным линиям, от утечки. Шифрование образует последний, практически непреодолимый «рубеж» защиты от НСД. Понятие «шифрование» часто употребляется в связи с более общим понятием криптографии. *Криптография*включает способы и средства обеспечения конфиденциальности информации (в том числе с помощью шифрования) и аутентификации.

*Конфиденциальность*– защищенность информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В свою очередь *аутентификация*представляет собой установление подлинности различных аспектов информационного взаимодействия: сеанса связи, сторон (идентификация), содержания (имитозащита) и источника (установление авторства с помощью цифровой подписи).

Число используемых программ шифрования ограничено, причем некоторые из них являются стандартами де-факто или де-юре. Однако даже если алгоритм шифрования не представляет собой секрета, произвести дешифрование (расшифрование) без знания закрытого ключа чрезвычайно сложно. Это свойство в современных программах шифрования обеспечивается в процессе многоступенчатого преобразования исходной открытой информации (plain text в англоязычной литературе) с использованием ключа (или двух ключей – по одному для шифрования и дешифрования). В конечном счете, любой сложный метод (алгоритм) шифрования представляет собой комбинацию относительно простых методов.

**Классические алгоритмы шифрования данных.**Имеются следующие «классические» методы шифрования:

• подстановка (простая – одноалфавитная, многоалфавитная одно-петлевая, многоалфавитная многопетлевая);  
Подстановка предполагает использование альтернативного алфавита (или нескольких) вместо исходного.

• перестановка (простая, усложненная);  
***Перестановка***потенциально обеспечивает большую по сравнению с подстановкой устойчивость к дешифрованию и выполняется с использованием цифрового ключа или эквивалентного ключевого слова, как это показано на следующем примере. Цифровой ключ состоит из неповторяющихся цифр, а соответствующее ему ключевое слово – из неповторяющихся символов. Исходный текст (plain text) записывается под ключом построчно. Зашифрованное сообщение (cipher text) выписывается по столбцам в том порядке, как это предписывают цифры ключа или в том порядке, в котором расположены отдельные символы ключевого слова.

• гаммирование (смешивание с короткой, длинной или неограниченной маской).  
***аммирование***(смешивание с маской) основано на побитном сложении по модулю 2 (в соответствии с логикой ИСКЛЮЧАЮЩЕЕ ИЛИ) исходного сообщения с заранее выбранной двоичной последовательностью (маской).

20.

Современное состояние телекоммуникационных сетей можно определить термином «движение к совершенству». Вряд ли можно предугадать, как они будут выглядеть в будущем, сколько поколений сетей и технологий предстоит еще пройти. Однако уже сегодня видны первые наработки: мощные сети передач и коммутации пакетов, высокоскоростные линии доступа, оптические телекоммуникационные технологии и т. д., которые и определяют следующие поколения телекоммуникационных сетей.

21.

Под **архитектурой компьютера** понимается его логическая организация, структура и ресурсы, т.е. средства вычислительной системы, которые могут быть существенны для программиста и пользователя компьютера. По сути, архитектура включает характеристики основных ресурсов компьютера, доступных программисту и пользователю.

Традиционная структура ЭВМ, изобретенная Фон Нейманом состоит из трех принципиально важных устройств: **памяти, устройства управления (УУ) и арифметически-логического устройства (АЛУ).**Эта структура и воплотила в себе основополагающие архитектурные идеи ЭВМ (архитектура Фон Неймана).

Эти идеи дополнялись важными принципами, которые позволили практически осуществить работу ЭВМ.

1.**Принцип программного управления работой ЭВМ**. Программы состоят из последовательности команд. Все типа команд в совокупности образуют машинный язык.

2. **Принцип условного перехода**. Это возможность перехода на тот или иной участок программы в зависимости от промежуточных результатов работы программы. Это позволило организовать циклическую обработку данных и итерационные алгоритмы вычислений. Благодаря этому число команд в программе может быть существенно сокращено.

3. **Принцип хранения программы в памяти машины.** Он позволил достигнуть принципиальной универсальности компьютера. Ибо алгоритмы обработки данных задаваемые программой можно легко изменять, используя перезапись программы в памяти компьютера.

4. **Принцип использования двоичной системы счисления**. Он обеспечил возможность использования широкого спектра физически по разному устроенных и технологически реализуемых устройств для хранения, обработки данных.

**5. Принцип** **иерархичности запоминающих устройств**. Это позволило решить дилемму объема памяти и ее быстродействия. Дело в том, что увеличение объема памяти уменьшает ее быстродействие. При этом, АЛУ обладает большим быстродействием, чем память с достаточным для практической работы компьютера объемом. Для этого память компьютера представляла набор иерархически связанных запоминающих устройств. Ближайшая к АЛУ запоминающее устройство обладало небольшим объемом, но было выполнено на тех же элементах что и арифметические и логические устройства в АЛУ.

22.

**Системная шина**(системная магистраль или системный интерфейс)**.** Это основная интерфейсная система компьютера, обеспечивающая сопряжение и связь всех его устройств между собой.

Интерфейс (interface) - совокупность средств сопряжения и связи отдельных устройств компьютера, обеспечивающая их эффективное взаимодействие.

Системная шина включает в себя:

* шину данных (ШД), содержащую провода (линии) и схемы сопряжения для параллельной передачи всех разрядов двоичного кода (машинного слова) операнда;
* шину адреса (ША), включающую провода и схемы сопряжения для параллельной передачи всех разрядов кода адреса ячейки основной памяти или кода адреса порта ввода-вывода внешнего устройства;
* шину управления (инструкций) (ШУ), содержащую провода и схемы сопряжения для передачи управляющих сигналов (импульсов) во все блоки машины (в частности управление обменом данных, передача запросов на прерывание и т.д.);

Порт ввода-вывода (I/O ≈ Input/Output port) – это пункт системного интерфейса, через который МП обменивается информацией с другим устройством ПК. Порты ввода-вывода – это абстрактное понятие. По аналогии с ячейками основной памяти их можно рассматривать как ячейки, через которые можно записать во внешнее устройство или, наоборот, прочитать из него. Так же как и ячейки памяти, порты имеют уникальные номера – адреса портов ввода-вывода. Ячейки памяти с этими адресами являются частью контроллера внешнего устройства, использующего этот порт, а не частью основной памяти компьютера.