ЛЕКЦИЯ № 10

ТЕМА 5: Информационные технологии и основы автоматизированных систем

УЧЕБНЫЕ ВОПРОСЫ

1. Высокопроизводительные вычислительные системы. Мультипроцессорные вычислительные системы
2. Защита информации в автоматизированных системах

ЛИТЕРАТУРА

1. Андреев А.И. Автоматизированные системы и связь в пожарной охране : учеб. пособие / А.И. Андреев, М.Х. Ахтямов. – Хабаровск.: Издательство ДВГУПС, 2008

2. Зыков В.И. и др.Автоматизированные системы управления и связь : учебник / В.И. Зыков, А.В Командиров, А.Б Мосягин, И. М Тетерин, Ю.В Чекмарёв; под общ. ред. профессора В.И. Зыкова. – М.: Академия ГПС МЧС России, 2006

1. Высокопроизводительные вычислительные системы. Мультипроцессорные вычислительные системы

Вычислительная система (ВС) представляет собой совокупность взаимосвязанных и взаимодействующих процессоров или ЭВМ, периферийного оборудования и программного обеспечения, предназначенную для сбора, хранения, обработки и распределения информации. Отличительной особенностью ВС является наличие в них нескольких вычислителей, реализующих параллельную обработку.

Параллелизм в вычислениях в значительной степени усложняет управление вычислительным процессом, использование технических и программных ресурсов.

При проектировании ВС реализуются следующие принципы:

- возможность работы в разных режимах;
- модульность структуры технических и программных средств;
- унификация и стандартизация технических и программных решений;
- способность систем к адаптации, самонастройке, самоорганизации;
- обеспечение необходимым сервисом пользователей при выполнении вычислений;
- иерархия в организации и управления процессом.

По типу вычислительные системы делятся на многомашинные и многопроцессорные.

Для повышения производительности, надёжности и достоверности вычислений используются многомашинные вычислительные системы (ММС). Комплекс таких машин схематически показан на рис.1 . Положения 1и 3 электронного ключа (ЭК) обеспечивают режим повышенной надёжности. При этом одна из машин выполняет вычисления, а другая находится в холодном или горячем резерве. Положение 2 электронного ключа соответствует событию, когда обе машины обеспечивают параллельный режим вычислений. При этом возможны два варианта вычислений:

• обе машины решают одну и ту же задачу и периодически сверяют результаты решений. Такой способ обеспечивает режим наибольшей достоверности, уменьшается вероятность появления ошибок в результате вычислений;

• обе машины работают параллельно, но обрабатывают собственные потоки заданий. Возможность обмена информацией между машинами сохраняется. Такой способ включения ЭВМ обеспечивает высокую производительность и используется в практике организации работ в крупных вычислительных центров, оснащённых несколькими ЭВМ высокой производительности.

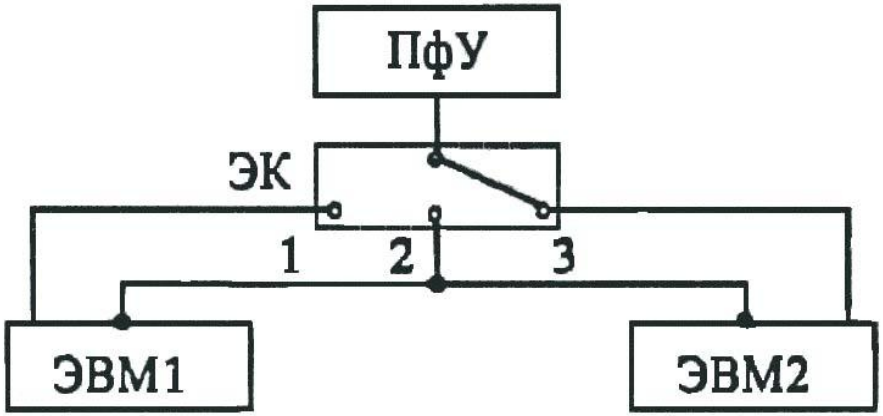


Рис. 1 Многомашинные комплексы

Схема, представленная на рис. 1 используется в различных модификациях при проектировании специализированных ММС. Основные различия ММС заключаются, как правило, в организации связи и обмена информацией между ЭВМ комплекса. Каждая из них сохраняет возможность автономной работы и управляется собственной операционной системой. Любая другая подключаемая ЭВМ комплекса рассматривается как специальное периферийное оборудование. В зависимости от территориальной разобщённости ЭВМ и используемых средств сопряжения обеспечивается различная оперативность их информационного сопряжения.

Многопроцессорные системы (МПС) строятся при комплексировании нескольких процессоров (рис.2). В качестве общего ресурса они имеют общую оперативную память (ООП). Параллельная работа процессоров и использование ООП обеспечивается под управлением единой операционной системы. При использовании такой схемы, по сравнению с ММС, обеспечивается наивысшая оперативность взаимодействия вычислителей – процесс

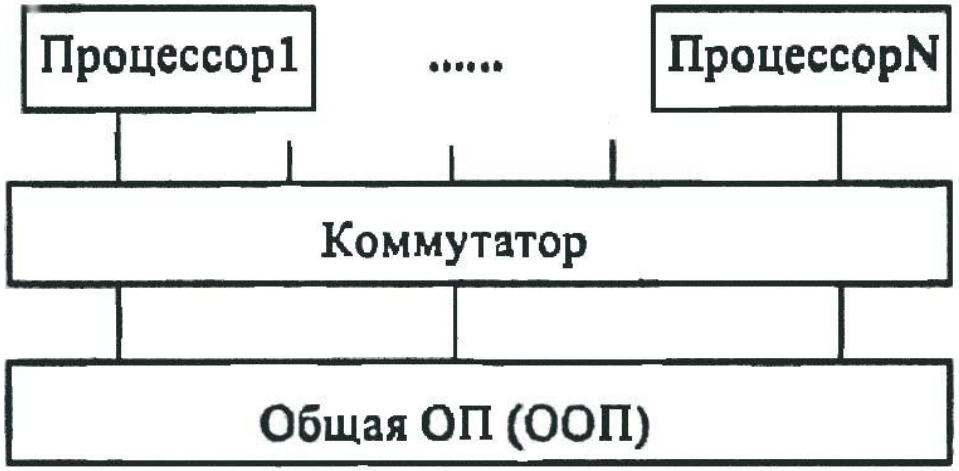


Рис. 2 Многопроцессорные системы

Многопроцессорные системы имеют недостатки. Эти недостатки связаны с использованием ресурсов общей оперативной памяти. При большом количестве комплексируемых процессоров возможно возникновение конфликтных ситуаций, когда несколько процессоров обращаются с операциями типа <<чтение >> и <<запись>> к одним и тем же областям памяти. Помимо процессоров к ООП подключаются все каналы (процессоры ввода – вывода), средства измерения времени и так далее, то есть возникает проблема коммутации абонентов и доступа их к ООП. Решение этой проблемы обеспечивается с помощью аппаратно – программных средств. Необходимо отметить, что процедуры взаимодействия усложняют структуру операционной системы МПС и от того, как они решаются во многом зависит эффективность применения многопроцессорных систем.

Кластер – это несколько компьютеров (узлов кластера), соединённых коммуникационными каналами и разделяющих общие ресурсы. Кластер имеет общую файловую систему и пользователем воспринимается как единый компонент.

Надёжность работы кластера обеспечивается программами, регулирующими скоординированное использование общекластерных ресурсов, обмен информацией между узлами кластера и осуществляющими взаимный контроль работоспособности этих узлов.

Каждый работающий в кластере компьютер может взять на себя дополнительную нагрузку отказавшего узла.

Кластеры обеспечивают высокую готовность системы (до 0,999) возможность наращивания производительности за счёт установки нового оборудования или замены устаревшего.

Кластерные системы используют специальные программы, обеспечивающие оптимальное распределение ресурсов и удобное администрирование:

- программы, выполняющие обнаружение и корректировку системных сбоев;
- программы, обеспечивающие непротиворечивость доступа приложений с разных компьютеров к общим ресурсам;
- программные модули управления дисковыми томами.

В случае возникновения отказов кластерная система выполняет:

- идентификацию отказов;
- формирование нового кластера;
- запуск контрольных программ;
- тестирование файловой системы.

Оптические компьютеры

В 2003 году компания **Lenslet** создала первый в мире оптический процессор. Процессор назывался EnLight256, его производительность составляла 8 терафлопс (триллионов арифметических операций в секунду)[0.1терафлопс]. Оптический компьютер просматривает за 1 секунду 80 000 страниц обычного ASCII-текста (**American Standard Code** for **Information Interchange**) . Операции выполнялись за счет манипуляции потоков света, а не электронов.

Преимущества оптической технологии:

- возможность использовать совершенно разные среды передачи, хранения и обработки информации;
- возможность обработки информации во время ее передачи через оптическую систему, которая реализует вычислительную среду;

возможность передавать информацию, которая закодирована оптическим лучом, практически без потерь энергии;

-отсутствие вероятности перехвата информации (по оптической технологии в окружающую среду ничто не излучается).

Оптический процессор

2. Защита информации в автоматизированных системах

Информационная безопасность является составной частью информационных технологий. Под информационной безопасностью понимается защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, направленных на нанесение ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

В обеспечении информационной безопасности выделяются следующие категории: доступность, целостность, конфиденциальность.

Доступность это возможность за приемлемое время получить требуемую информационную услугу. Целостность информации представляет собой свойство информации сохранять свою структуру и содержание в процессе передачи и хранения. Конфиденциальность информации – это свойство информации быть доступной только ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.

Для защиты информации в организации реализуется политика безопасности, которая представляет собой совокупность норм, правил и практических рекомендаций, регламентирующих работу компьютерной системы (сети) от заданного множества угроз безопасности. В настоящее время применяют следующие технологии информационной безопасности :

- комплексный подход, обеспечивающий рациональное сочетание технологий и средств информационной защиты;
- применение защищённых виртуальных частных сетей (VPN) для защиты информации, предаваемой по открытым каналам связи;
- криптографическое преобразование данных для обеспечения целостности, подлинности и конфиденциальности информации;
- применение межсетевых экранов для защиты вычислительной сети от внешних угроз при подключении к общедоступным сетям связи;

- управление доступом на уровне пользователей и защита от несанкционированного доступа к информации;
- гарантированная идентификация пользователей путём применения токенов (touch – memory, ключи для USB и так далее);
- поддержка инфраструктуры управления открытыми ключами (PKI);
- защита информации на файловом уровне путём шифрования файлов и каталогов;
- защита от вирусов с использованием специализированных комплексов профилактики и защиты;
- технологии обнаружения вторжений (Intrusion Detection) и активного исследования защищённости информационных ресурсов;

• централизованное управления средствами информационной безопасности.

Виртуальной защищённой сетью VPN называют объединение локальных сетей и и отдельных компьютеров через открытую внешнюю среду передачи информации в единую корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

Сеть VPN формируется путём построения виртуальных защищённых каналов связи, создаваемых на базе открытых каналов связи общедоступной сети(Рис.3).

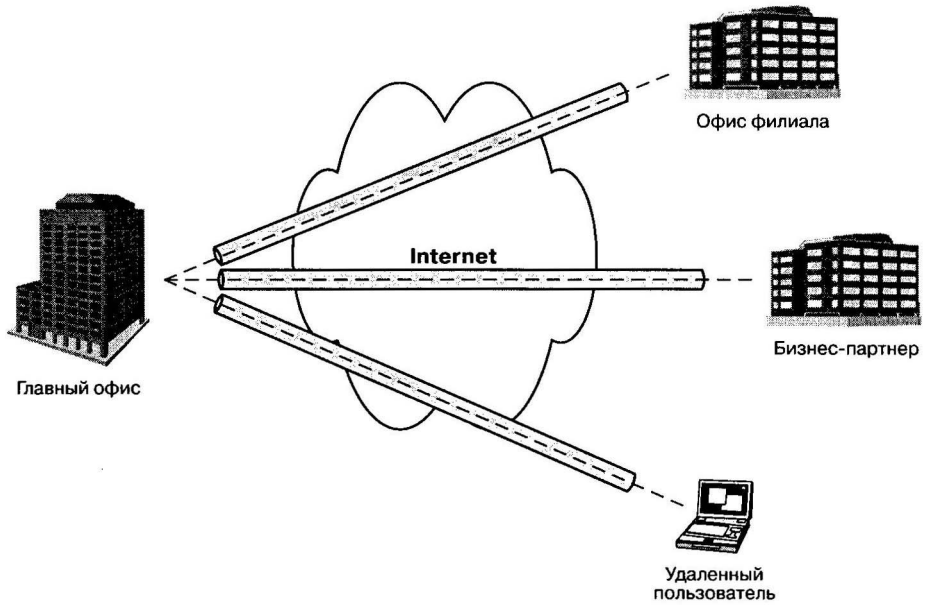


Рис. 3. Виртуальная защищённая сеть

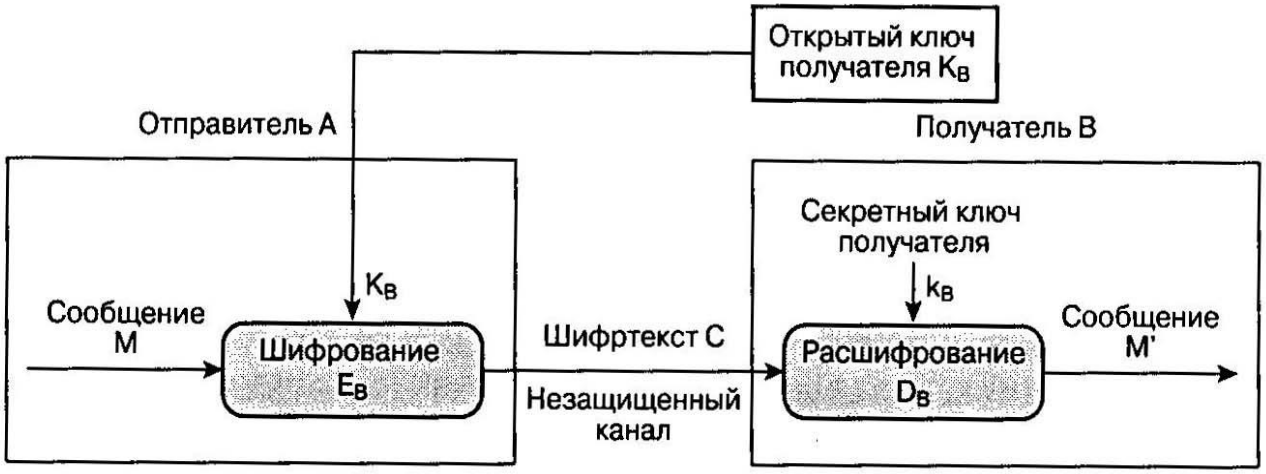
Виртуальные защищённые каналы называются туннелями.

Туннель VPN представляет собой соединение, проведённую через открытую сеть, по которому передаются криптографически защищённые пакеты сообщений виртуальной сети. Защита информации в процессе её передачи по туннелю VPN основана на выполнении следующих функций.

- аутентификации взаимодействующих сторон;
- криптографического закрытия передаваемых данных;
- проверки подлинности и целостности доставляемой информации.

В ассиметричной системе шифрования для шифрования информации и её расшифрования используются различные ключи.

- открытый ключ *K* используется для шифрования информации, вычисляется из секретного ключа *k*;
- секретный ключ *k* используется для расшифрования информации, зашифрованной с помощью парного ему открытого ключа *K*.



Обобщенная схема асимметричного шифрования

Для противодействия несанкционированному межсетевому доступу МЭ располагается между защищаемой сетью организации и внешней средой. При этом всё взаимодействие между этими сетями осуществляется через МЭ. Организационно МЭ входит в состав защищаемой сети.

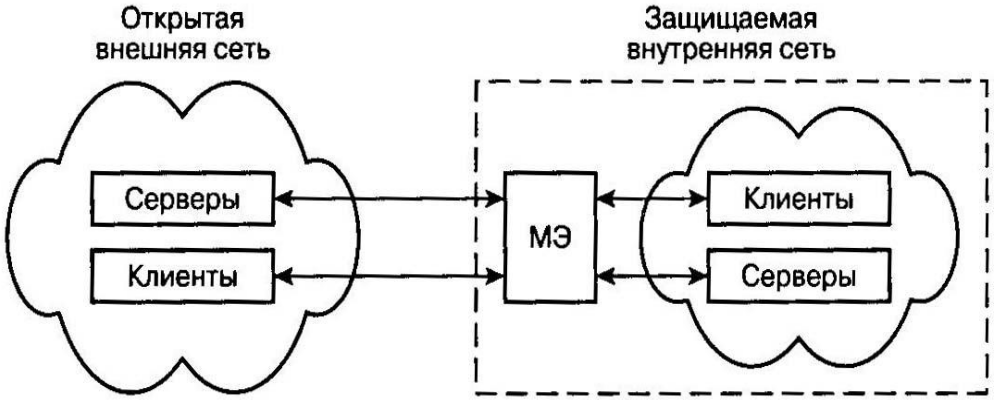


Схема подключения межсетевого экрана

МЭ решает следующие задачи:

- ограничение доступа внешних пользователей к внутренним ресурсам корпоративной сети;
- разграничение доступа пользователей защищаемой сети к внешним ресурсам.

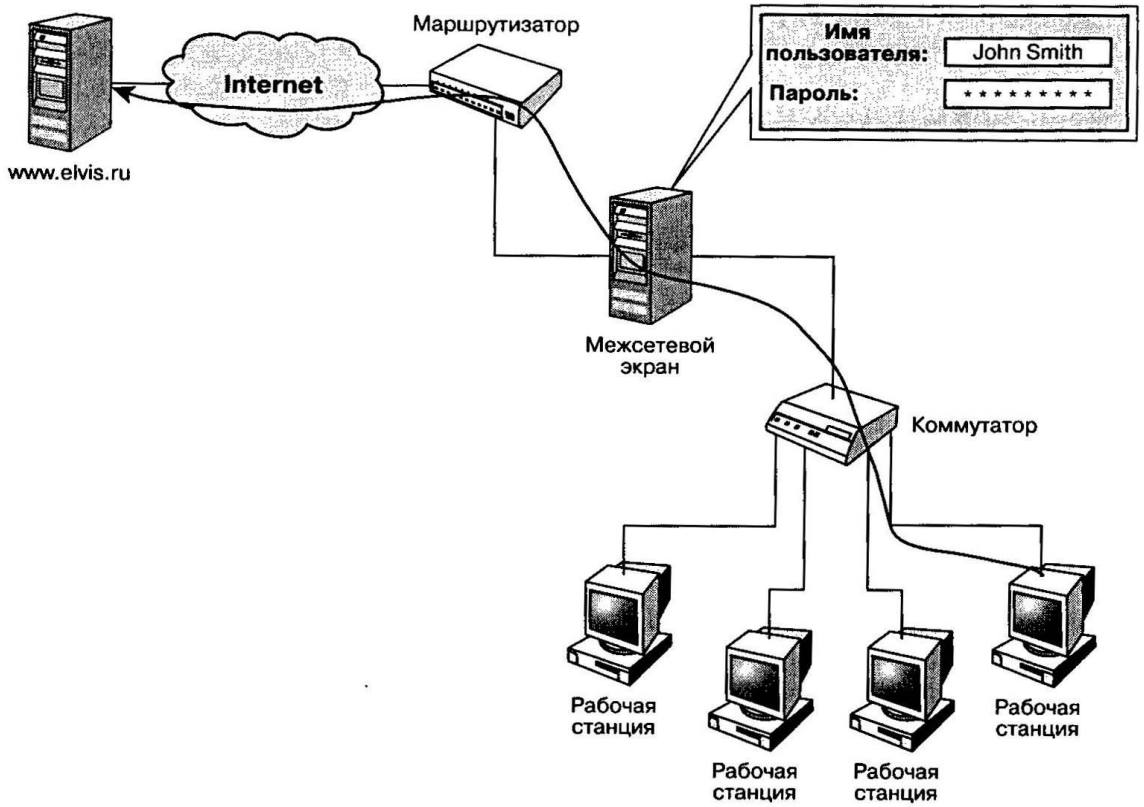


Схема аутентификации пользователя по предъявляемому паролю

Эффективным средством повышения надёжности защиты данных на основе гарантийной идентификации пользователя являются электронные токены, которые являются своего рода контейнерами для хранения персональных данных пользователя системы. Эта информация всегда находиться на носителе и предъявляется только во время доступа к системе или компьютеру.

При большом числе пользователей схемы аутентификации на основе индивидуальных паролей не всегда эффективны так как требуют ввода в систему и хранение каждого пароля. Для повышения эффективности АС используются технологии аутентификации на основе цифровых сертификатов стандарта X.509 и PKI.

Сертификаты позволяют разделить пользователей на несколько категорий и предоставлять разные права доступа в зависимости от принадлежности пользователя к определённой категории. Инфраструктура управления открытыми ключами PKI служит для обеспечения жизненного цикла сертификатов и позволяет, в частности, удостовериться в подлинности предъявленного сертификата за счёт проверки подлинности цифровой подписи сертифицирующей организации или цепочки

Важным элементом комплексной защиты информации является антивирусная защита. Защищённый трафик не может контролироваться антивирусными средствами. Поэтому эти средства устанавливаются в узлах, на которых информация храниться, обрабатывается и передаётся в открытом виде.

Средства обнаружения вторжений позволяют повысить уровень защищённости вычислительной сети и хорошо дополняют защитные функции межсетевых экранов. Если межсетевые экраны отсекают потенциально опасный трафик и не пропустить его в защищаемые сегменты, то средства обнаружения вторжений анализируют результирующий трафик в защищаемых сегментах и выявляют атаки на ресурсы сети или потенциально опасные действия. Кроме того, они могут использоваться в незащищённых сегментах, например, перед межсетевыми экранами, для получения общей картины об атаках, которым подвергается сеть извне.

Централизованное управление средствами безопасности предполагает наличие единой политики безопасности организации. Каждое устройство защиты, работающее в информационной системе организации, должно поддерживать взаимодействие с централизованной системой управления и получать от неё защищённым образом правила локальной политики безопасности, относящиеся к данному устройству. Наличие централизованных средств управления продуктами безопасности является обязательным требованием для возможности их применения в организации.