Техническое, программное и сетевое обеспечение информационных систем

1.5 Информационное обеспечение автоматизированных рабочих мест

Обеспечение автоматизированных рабочих мест информацией выполняется с помощью системы управления базами данных, которая позволяет хранить, представлять и преобразовывать по запросу.

База данных – это совокупность взаимосвязанных данных, которую можно использовать оптимальным образом для одного или нескольких приложений в определенной предметной области человеческой деятельности.

Каждая из систем управления базами данных (СУБД) основывается на определенной модели, отражающей взаимосвязи между объектами. Существуют иерархические, сетевые и реляционные модели данных. Большинство современных СУБД используют реляционную модель. С помощью такой модели могут быть представлены объекты предметной области и взаимосвязи между ними.

Использование базы данных обеспечивает независимость данных и программ, реализацию отношений между данными, совместимость компонентов БД, простоту изменения логической и физической структур БД, целостность, восстановление и защиту БД и др.

К другим целям использования БД относятся: сокращение избыточности в хранимых данных, устранение несовместимости в хранимых данных с помощью автоматической корректировки и поддержки всех дублирующих записей, уменьшение стоимости разработки программ, а также программирование запросов к БД.

Перенос программ управления данными с рабочих станций на сервер способствует высвобождению ресурсов рабочих станций, предоставляет возможность увеличить число частных, локально решаемых задач. Это централизует важные функции управления данными, таких как защита информации баз данных, обеспечение целостности данных, управление совместным использованием ресурсов.

Одним из важных преимуществ архитектуры клиент-сервера в распределенной обработке данных является возможность сокращения времени реализации запроса. В подтверждение этому рассмотрим две базовые технологии обработки информации в архитектуре клиент-сервера сети и технологии использования традиционного файлового сервера.

Если прикладная программа БД загружена на рабочую станцию и пользователю необходимо получить все записи, удовлетворяющие некоторым поисковым условиям, то в среде традиционного файлового сервера программа управления данными, которая выполняется на рабочей станции, должна осуществить запрос к серверу каждой записи БД (рисунок 1.11).

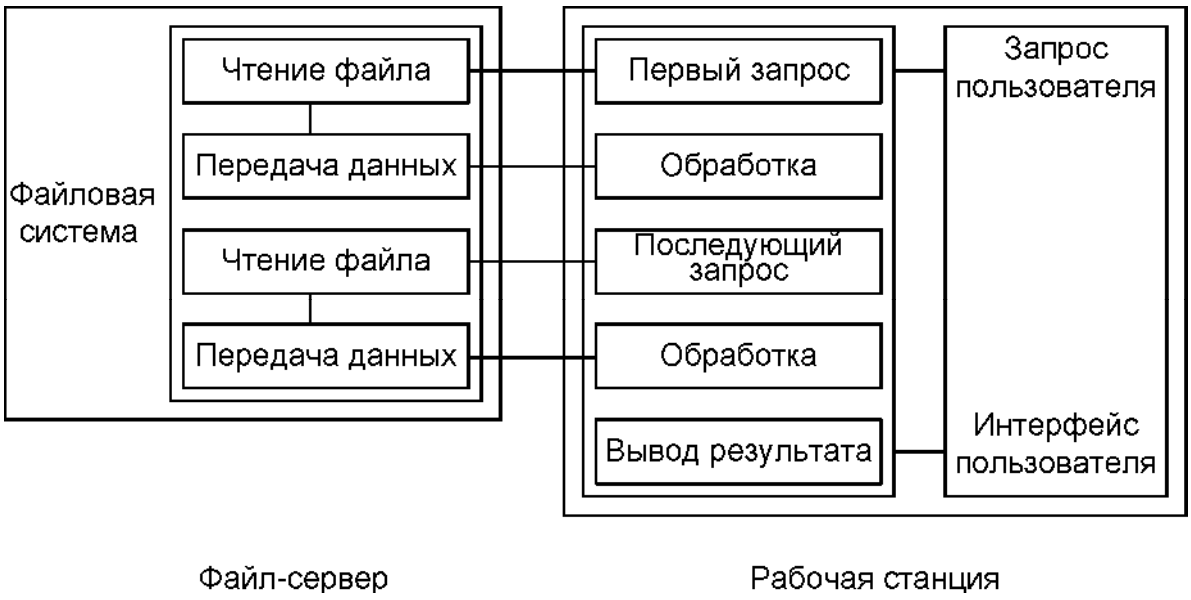

Рисунок 1.11 – Типовая среда обработки запросов в сетях ЭВМ

Программа управления данными на рабочей станции может определить, удовлетворяет ли запись поисковым условиям, лишь после того как она будет передана на рабочую станцию. Данный вариант обработки информации имеет наибольшее суммарное время передачи данных по каналам сети.

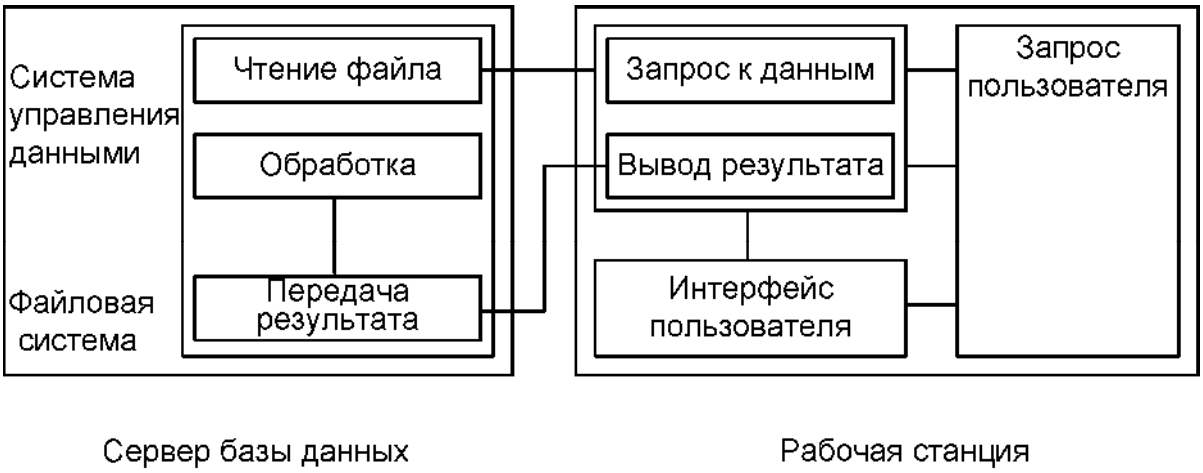

Рисунок 1.12 – Распределенная среда обработки запросов в сетях ЭВМ

В среде клиент-сервера, напротив, рабочая станция посылает запрос высокого уровня серверу БД. Сервер БД осуществляет поиск записей на диске и анализирует их. Записи, удовлетворяющие условиям, могут быть накоплены на сервере. После того как запрос целиком обработан, пользователю на рабочую станцию передаются все записи, которые удовлетворяют поисковым условиям (рисунок 1.12).

Данная технология позволяет снизить сетевой трафик и повысить пропускную способность сети. Более того, за счет выполнения операции доступа к диску и обработки данных в одной системе сервер может осуществить поиск и обрабатывать запросы быстрее, если бы эти запросы обрабатывались на рабочей станции.

Работа пользователей с распределенными базами данных имеет ряд особенностей, тем более что некоторые данные могут дублироваться. Выгоды, получаемые от дублирования, пропорциональны соотношению объемов выборки данных и их обновления. Для поддержания целостности БД требуется корректировка всех копий. Наличие копий приводит к увеличению стоимости хранения и обновления информации, но так повышается устойчивость системы при отказах.

1.6 Особенности построения современных информационных систем

Актуальность проблемы хранения и оперативного поиска данных привела к появлению такого понятия, как хранилище данных. Следует упомянуть о необходимости использования единых информационных хранилищ в аналитических системах и в первую очередь в системах поддержки принятия решений (СППР). СППР пользуются информацией, собранной с помощью компьютерных сетей из множества систем обработки данных (СОД). Данные в СОД собираются, хранятся и по достижении установленного срока выгружаются. В различных СОД данные могут не быть согласованы между собой, информация в них может быть по-разному структурирована, степень ее достоверности определить сразу бывает достаточно трудно. Все это свидетельствует о том, что архивные данные из СОД без предварительной доработки использовать в информационных хранилищах нецелесообразно.

Информационные хранилища для СППР должны обладать некоторыми специфическими свойствами. От них требуется хранение информации в хронологическом порядке, так как без отражения хронологии данных нельзя говорить о решении задач прогнозирования и анализа тенденций (основных задач СППР). Важнейшее требование, предъявляемое к информационным хранилищам – это достоверность информации, которую без согласованности данных обеспечить невозможно.

Задача создания информационных хранилищ чрезвычайно сложна, и достаточно часто ее решение связано с рядом проблем.

Хранилища данных работают с внешними источниками, т. е. различными информационными системами, электронными архивами, каталогами и справочниками, статистическими сборниками и т. д. Все внешние источники реализованы на основе различных программных и аппаратных средств. На основе этих разнородных средств и решений необходимо построить единую информационную, функционально согласованную систему.

При выборе СУБД следует учитывать, что скорость работы в сети зависит не только от аппаратных возможностей оборудования, но и в значительной степени от программного обеспечения (ПО). В классической сетевой технологии БД хранится на сервере.

Программы исполняются на рабочих станциях, данные поступают по сети. При локальной работе с базами особенных проблем не возникает. Но когда к таблицам пытаются обратиться по сети одновременно несколько пользователей, возникают трудности. В рамках этой технологии два и более пользователя не могут одновременно изменить одни и те же данные.

При использовании технологии «клиент-сервер» стали создаваться распределенные системы. Современные серверы баз данных (*Oracle*, *Sybase*, *Informix*, *Interbase* и т. д.) способны переносить часть нагрузки на сервер. Так, возможно выполнение хранимых на сервере процедур, запускаемых как с клиентской части программы, так и с серверной. Однако, несмотря на улучшение эксплуатационных параметров, уменьшение сетевого трафика не очень значительно. К тому же программы все равно должны исполняться на мощных рабочих станциях.

1.7 Техническое обеспечение информационных систем

На информационном уровне все автоматизированные рабочие места предприятия тесно связаны между собой, поэтому для эффективной информационной системы необходима локальная компьютерная сеть для исключения возможности рассогласования данных на персональных компьютерах предприятия.

Локальные сети различаются по типу кабеля и по своей конфигурации (рисунок 1.13).

Итак, для связи компьютеров в локальную сеть используется три типа носителя информации: коаксиальный кабель, провод типа «витая пара» и оптическое волокно.

Коаксиальный кабель представляет собой одножильный провод с медной оплеткой. Длина сегмента сети для этого кабеля не может превышать 180 м, а скорость обмена информации ограничивается 10 Мбит. При этом не требуется никакого дополнительного оборудования. Правда, если длина сети будет превышать 180 м, то придется устанавливать дополнительные устройства (сетевые повторители – репитеры) через каждые 180 м. На сегодняшний день это самый дешевый носитель. Однако эта дешевизна довольно обманчива. Дело в том, что сеть, построенная на коаксиальном кабеле, требует довольно жестких правил подключения компьютеров в электрическую сеть. Все компьютеры должны быть заземлены.

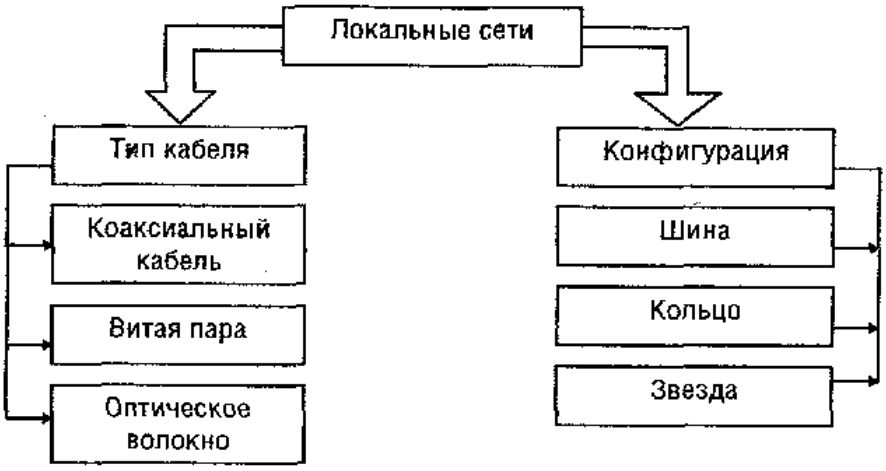

Рисунок 1.13 – Классификация локальных компьютерных сетей

Данный вид носителя используется в том случае, когда с минимальными затратами нужно соединить в сеть небольшое число компьютеров в небольшой транспортной компании.

Витая пара представляет собой многожильный провод в общей пластиковой оболочке. Длина сегмента сети для этого кабеля не может превышать 100 м, а скорость обмена информацией доходит до 100 Мбит (в 10 раз выше, чем по коаксиальному кабелю). При этом для стыковки компьютеров в небольших сетях требуется дополнительные устройства сопряжения – так называемые «хабы» (*hub*). Большие и сильно разветвленные сети требуют маршрутизаторов, концентраторов и прочего оборудования. К одному устройству сопряжения может быть подключено, как правило, четыре, восемь, 16 компьютеров. Таким образом, при наличии одного устройства сопряжения максимальное расстояние между компьютерами не превысит 200 м. Сети, построенные на витой паре, менее зависимы от прихоти электрического питания компьютеров, более электробезопасны, быстры и надежны. Однако за надежность надо платить. Сеть на витой паре будет стоить дороже коаксиальной в 3–6 раз. Витая пара, несмотря на более высокую стоимость, постепенно вытесняет коаксиальный кабель, и это не дань моде, а гарантия стабильности и надежности работы сети.

Оптическое волокно – это принципиально другой тип носителя информации, обеспечивающий сверхбыструю передачу данных. Длина сегмента сети для этого кабеля может достигать двух километров, а скорость обмена информации доходит до 1

Гбит. При этом для стыковки компьютеров требуются дополнительные устройства сопряжения.

Локальная сеть, построенная на кабеле из оптического волокна, будет самой быстрой и надежной, но ее цена примерно в 10 раз превысит цену сети на базе витой пары. Основные затраты здесь придутся на устройства сопряжения (сам кабель стоит примерно в четыре раза дороже, чем витая пара). Конечно, строить всю сеть на данном носителе нецелесообразно, но применение оптического волокна во многих случаях вполне оправданно. Например, склад предприятия удален от административного здания на 600–800 м, диспетчерский пункт находится в двух километрах от АТП. В обоих случаях сегмент сети, расположенный между зданиями, может быть выполнен на оптическом волокне.

В сетях существует три схемы соединения компьютеров в сеть: шина, кольцо и звезда.

Шина (сеть *Ethernet*). В этом случае компьютеры соединяются последовательно через общий кабель (рисунок 1.14). На концы кабеля ставятся специальные «заглушки» (терминаторы).

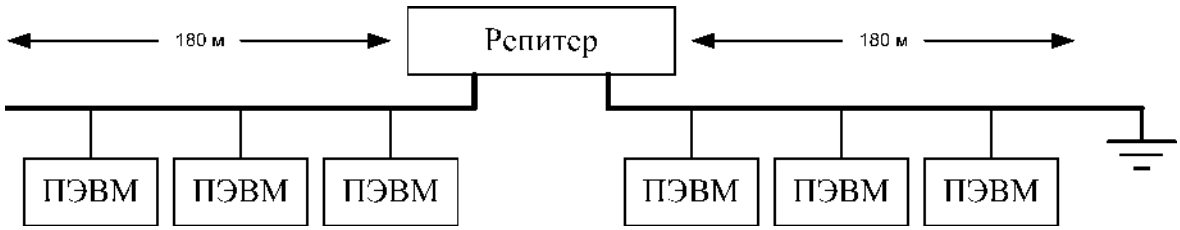

Рисунок 1.14 – Сеть типа «Шина»

При такой конфигурации сети будут минимальные затраты на кабель и монтажные работы. Однако такая топология сети имеет один существенный недостаток: если кабель обрывается в одном месте, то нарушается работа всей сети.

Кольцо (сеть *TokenRing*). В этом случае компьютеры также соединяются последовательно, но отпадает необходимость в терминаторах, так как кабель замкнут (рисунок 1.15).

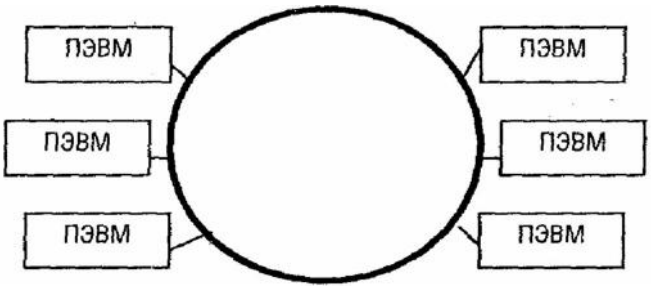

Рисунок 1.15 – Сеть типа «Кольцо»

При такой топологии разрыв кабеля также приводит к остановке всей сети.

Звезда (сеть *Ethernet*). При такой топологии сети расход кабеля значительно выше, чем в двух предыдущих вариантах (иногда в десятки раз), поскольку каждый компьютер соединяется с устройством сопряжения отдельным кабелем (рисунок 1.16). Однако это обеспечивает большую надежность, поскольку обрыв одного звена приводит к нарушению обмена информацией только с одним компьютером, остальные члены сети могут и не заметить обрыва. При работе с данными на первое место всегда ставится надежность, поэтому такая конфигурация достаточно популярна, несмотря на большие затраты.

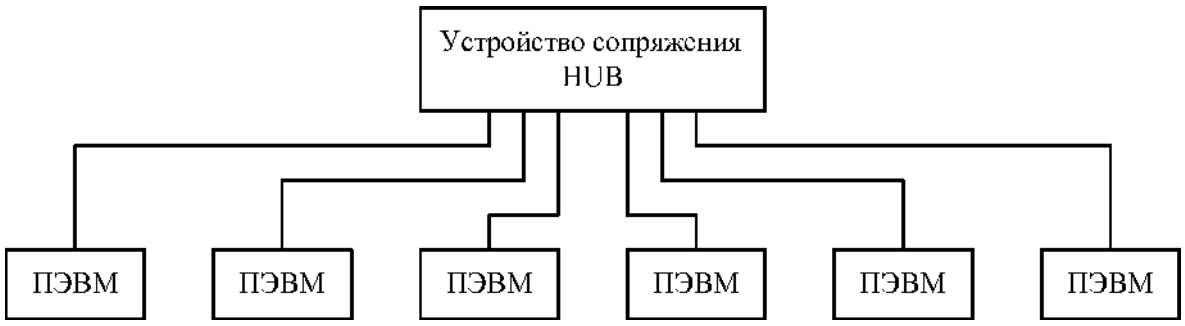

Рисунок 1.16 – Сеть типа «Звезда»

1.8 Программное обеспечение информационных систем

Любой компьютер без программного обеспечения обладает меньшим функционалом, чем арифмометр, последний хотя бы позволяет складывать и вычитать. В современном компьютере множество программ, готовых в любой момент времени выполнить свои функции. Программное обеспечение можно разделить на три группы: системное, инструментальное и прикладное (рисунок 1.17).

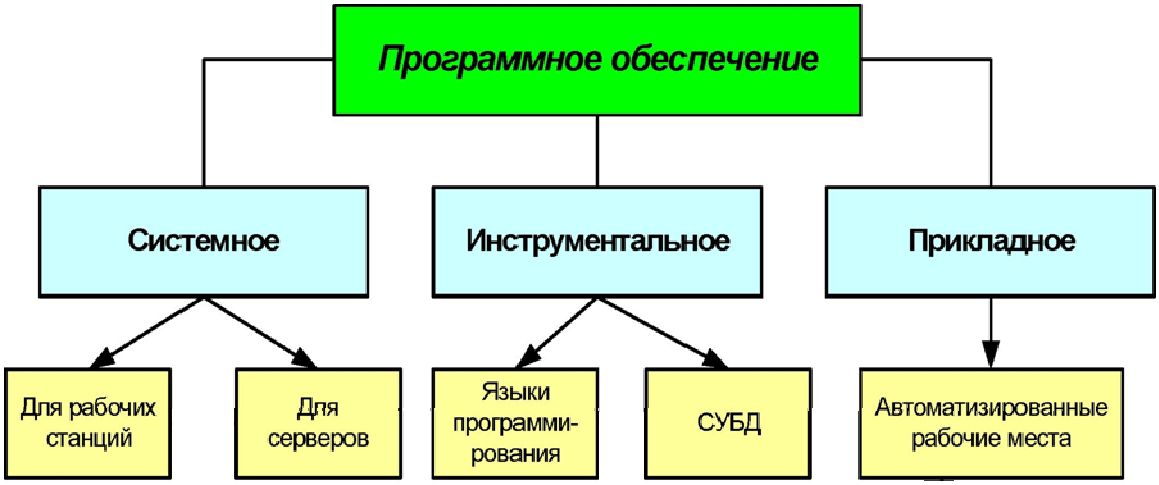

Рисунок 1.17 – Программное обеспечение

Приведенная схема не охватывает всего спектра используемых программ, однако позволяет дать общие представления о том, что должно быть установлено на компьютерах предприятия, чтобы специалисты могли получать адекватную информацию для своевременного принятия управляющих решений.

Операционная система – это набор программных средств, который начинает работать сразу после того, как включена кнопка электрического питания компьютера. Операционная система управляет работой компьютера, внешних устройств (принтеры, модемы) и обеспечивает работу прикладных программ.

Наиболее распространенной ОС является *Windows* (*Windows* 10, *Windows* 7, *Windows XP*). Это многозадачная система, позволяющая одновременно выполнять несколько процессов (ввод данных, расчет, печать и т. п.). Данная система обеспечивает связь между компьютерами без дополнительных программных средств.

Одним из основных преимуществ *Windows* является наличие многочисленного разнообразного программого обеспечения.

1.9 Сетевое программное обеспечение

При использовании операционной системы *Windows* нет необходимости в установке специальных сетевых программ, поскольку сетевые функции встроены в эту операционную систему.

Сети могут быть одноранговыми или с выделенным сервером. В одноранговой сети все компьютеры имеют «равные права», хотя один из них несет явно большие обязанности (на нем хранится база данных). Такой компьютер называют псевдосервер (рисунок 1.18).

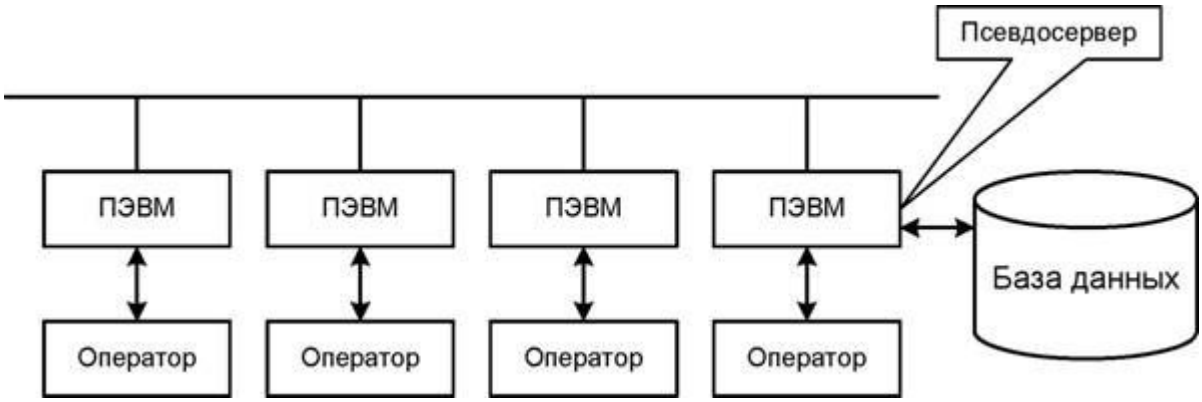

Рисунок 1.18 – Одноранговая сеть

Так как псевдосервер несет на себе двойную нагрузку (он работает как рабочая станция и предоставляет хранящиеся на нем данные другим пользователям сети) производительность одноранговой сети снижена.

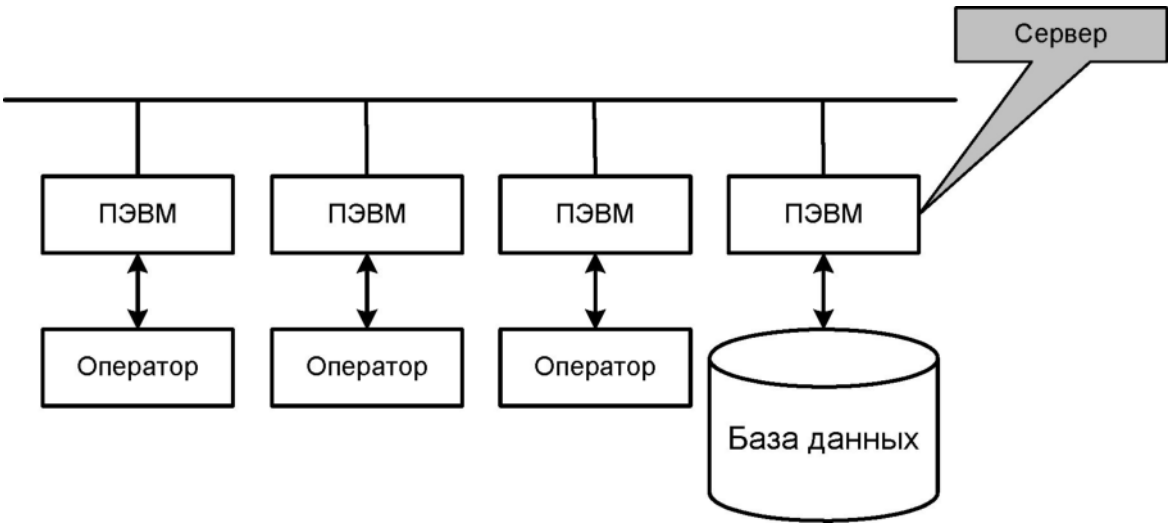

Рисунок 1.19 – Сеть с выделенным сервером

В сети с выделенным сервером один из компьютеров обеспечивает только хранение и обработку данных (рисунок 1.19). Он, как правило, имеет большую производительность, чем остальные компьютеры сети. Такое разделение функций вполне оправданно, так как обеспечивает лучшую производительность всех членов сети. Сервер может работать под управлением серверной версии операционной системы *Windows*.

1.10 Инструментальное программное обеспечение

К инструментальным средствам относятся системы управления базами данных (СУБД) и языки программирования. С помощью этого набора инструментов создается прикладное программное обеспечение, с которым работают пользователи компьютеров. От правильного выбора инструментальных средств во многом определяется надежность и эффективность вашей будущей информационной системы. Следует отметить, что некоторые инструментальные средства существуют сами по себе в «чистом» виде (язык программирования СИ, СУБД *MS SQL Server*).

СУБД обеспечивает хранение данных, а язык программирования дает возможность написать программную оболочку, посредством которой пользователь имеет возможность доступа к данным.

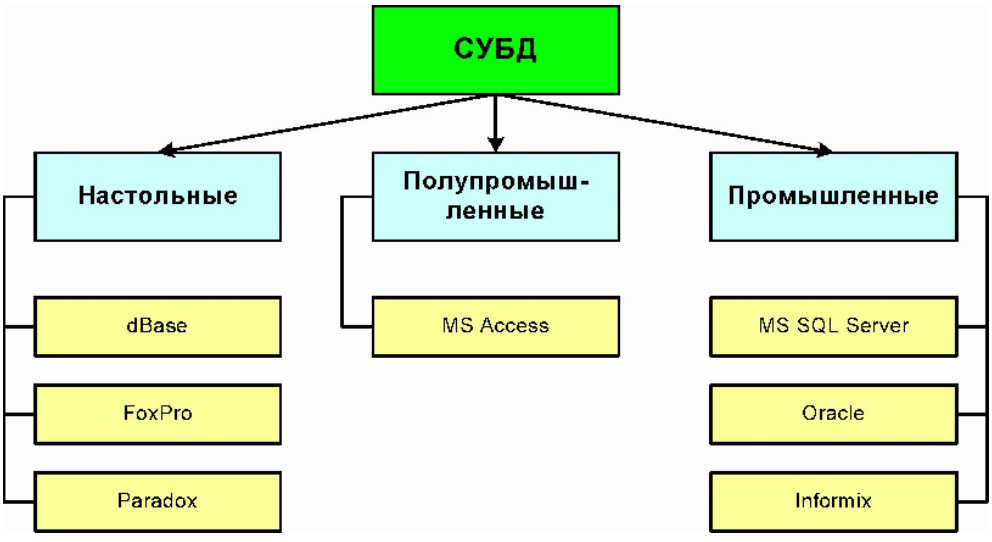

Рисунок 1.20 – Виды СУБД

От правильности выбора СУБД будет зависеть эффективность работы всей проектируемой системы. Все СУБД можно условно разбить на три класса (рисунок 1.20): настольные (малые базы для

одного компьютера или мелкой фирмы), полупромышленные (информационные базы для средних предприятий) и промышленные (информационные базы для крупных предприятий и государственных структур).

На сегодняшний день на транспортных предприятиях наибольшее распространение получили настольные СУБД, а для хранения данных чаще всего используется формат СУБД *dBase* (так называемые *DBF*-файлы). Они отличаются простотой, неприхотливостью к технике и системным программам, возможностью работать практически со всеми языками программирования. База данных в этом случае представляет собой некий открытый набор таблиц со свободным доступом к содержащимся в них данных. Кроме того, имеется набор вспомогательных индексных файлов, обеспечивающих быстрый поиск информации.

В настоящее время широкое распространение получила сравнительно новая локальная база данных *SQLite*, отличающаяся простотой и достаточной мощностью (Приложение 2). Чтобы использовать ее возможности следует поместить только один файл – библиотеку (*sqlite3.dll*) в папку с исполнительным файлом прикладной программы.

Никаких связей между таблицами не существуют (они временно создаются в период работы прикладных программ), целостность базы, поддержка индексных файлов зависит от программиста. Простота таких СУБД порождает массу существенных недостатков. В частности из-за своей открытости базы данных не имеют защиты от сознательного искажения информации. Заинтересованное лицо может с любого компьютера сети открыть нужный файл и подкорректировать данные в свою пользу (например, добавить водителю отработанных часов, увеличив тем самым ему зарплату). Такие базы склонны к разрушению в случае неожиданного отключения питания или сбоев в работе сети (чаще всего в этом случае нарушается структура индексных файлов). Нельзя похвастаться и быстродействием, по мере накопления информации скорость работы пользователей начинает замедляться. Кроме того, такие базы достаточно «рыхлые». Например, если под фамилию водителя в таблице отведено 20 символов, а к вам принят на работу водитель с фамилией, состоящей всего из двух букв (например Ли), то на

магнитных дисках будут храниться 18 ничего не значащих пробелов. Количество «пустот» может достигать 80 %. Такие базы довольно сложно сопровождать, поскольку количество разрозненных файлов в реально работающих в АТП системах доходит до 200 и выше.

Гораздо меньше проблем связано с эксплуатацией полупромышленных СУБД (например, *Access*). В этих СУБД сочетается простота настольных и надежность промышленных баз данных. У этих баз данных несколько иная структура (рисунок 1.21).

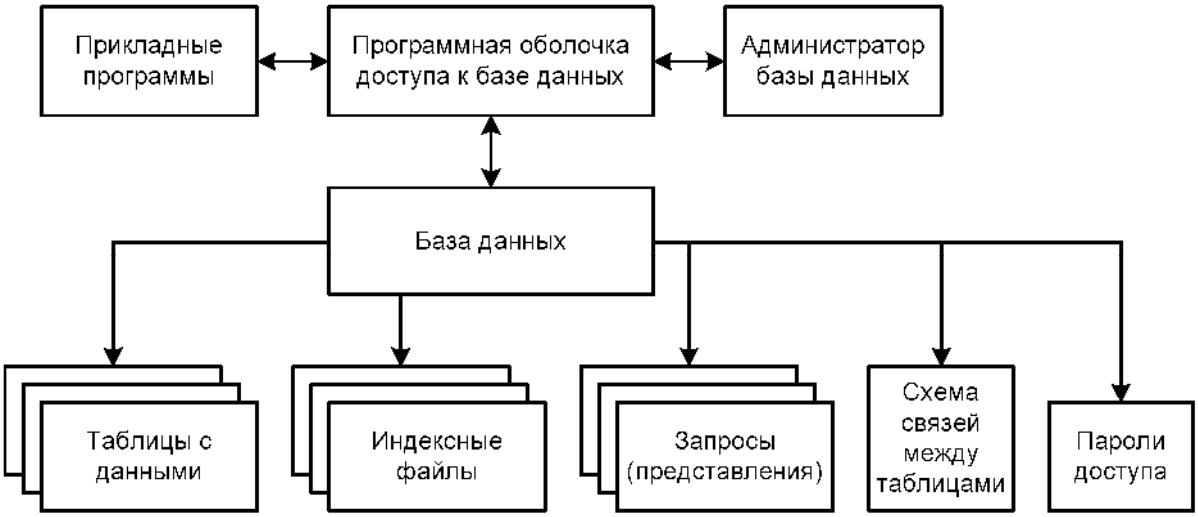

Рисунок 1.21 – Структура полупромышленной СУБД

Основным отличительным признаком этих СУБД является наличие некой программной оболочки, через которую осуществляется доступ ко всем внутренним элементам базы данных. Эта оболочка защищает информацию от любых внешних воздействий. Не имея паролей, никто не в состоянии испортить или исказить информацию. В базе данных хранятся ее внутренняя структура, связи между таблицами, обеспечивающие её целостность. Это очень важный момент, ведь даже программист во время написания и отладки прикладных программ не сможет испортить данные и нарушить структуру их целостности. От программиста и пользователя скрыты индексные файлы. СУБД сама создает их, обеспечивает сохранность и соответствие основным таблицам. Для выборки данных в полупромышленных СУБД используется универсальный язык *SQL*-запросов. Это единый стандарт языка практически для всех баз данных

независимо от производителя. *SQL*-запросы также могут храниться в самой СУБД, что обеспечивает идентичность выборки одинаковых данных с разных рабочих мест и высокую скорость обработки информации. Все отмеченные выше элементы хранятся на магнитном носителе в виде единственного файла, естественно упрощается процедура архивации и восстановления информации.

В полупромышленных СУБД используется механизм транзакций – отката назад в случае сбоев в работе системы (отключение питания, обрыв сетевого кабеля и пр.). Этот механизм обеспечивает дополнительную защиту информации от разрушения. Такие базы не хранят на дисках «пустоты», за счет этого они менее «рыхлые» по сравнению с настольными СУБД. За счет всего вышесказанного скорость выборки информации из связанных таблиц в 30–40 раз выше, чем в базах на *DBF*-файлах. Объём хранимых данных в полупромышленных СУБД может достигать 1–2 Гб.

Промышленные СУБД представляют вершину надежности и стабильности в работе (рисунок 1.22).

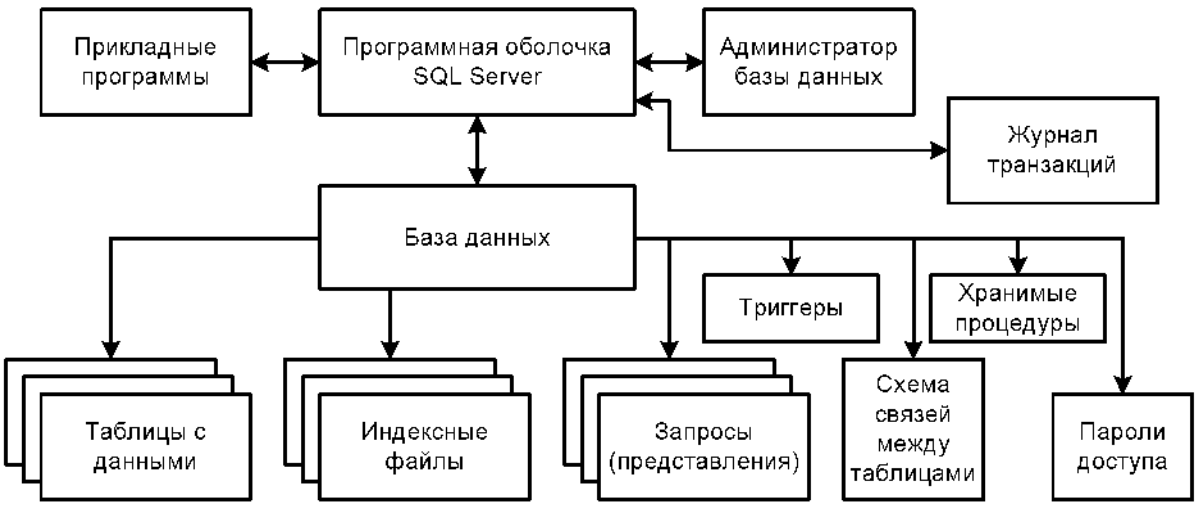

Рисунок 1.22 – Структура промышленной СУБД

Они обладают всеми отмеченными выше достоинствами полупромышленных СУБД и имеют ряд дополнительных возможностей.

Объем хранимых данных не ограничен, можно использовать хранимые процедуры и триггеры – фрагменты программного кода пользовательского приложения, хранимого и исполняемого на сервере. Постоянно ведется журнал транзакций – копии всех

изменений в базе данных, что дает возможность автоматически восстанавливать информацию в случаях нарушений электропитания или других сбоев в работе сети. Однако промышленные СУБД более «громоздки» и требуют наличия квалифицированного обслуживающего персонала.

Для разработки прикладного программного обеспечения можно использовать два типа языков программирования: интерпретаторы (*FoxPro*, *Centura*) и компиляторы (*Clipper*, *Delphi*, *Visual Basic*, СИ). При выборе языка программирования нужно учитывать следующие моменты: возможность работы с данными из различных СУБД, возможность создания *ActiveX* компонент (модулей программ, способных работать в неродной среде программирования), обеспечение хорошего быстродействия. На сегодняшний день реально создание информационной системы, отдельные модули которой написаны на разных языках (COM-технология).

К группе таких языков относятся СИ, *FoxPro*, *Delphi*, *Visual Basic*. Можно использовать любой из них. Однако нужно учесть, что *FoxPro* не является полноценным компилятором, а значит, готовое приложение будет работать медленнее. СИ – довольно мощный язык, но он в меньшей степени адаптирован для работы с базами данных. *Delphi* и *Visual Basic* являются полноценными компиляторами и имеют развитые средства для работы с широким спектром СУБД. Они наиболее приемлемы для создания прикладных программ для транспортных компаний. На *Delphi* обычно работает тот, кому ближе *Pascal*. *Visual Basic* – это базовый язык программирования фирмы *Microsoft*. Он продается в виде отдельного продукта, а также является составной частью всех офисных приложений (*Word*, *Excel*, *Access*, *Power Point*). Его чаще используют те, кто строит прикладные программы в тесной интеграции с офисными системами.

1.11 Прикладное программное обеспечение

Программные, сетевые, инструментальные программные средства обеспечивают функционирование прикладного программного обеспечения – автоматизированных рабочих мест.

Автоматизированные рабочие места являются результатом совместного труда программистов и инженерно-технического персонала. Эффективность работы информационной системы будет

зависеть от двух основных факторов: насколько грамотно сформулировано техническое задание на систему, подобраны инструментальные средства и СУБД. Только в результате совместного труда этих двух категорий работников может быть создано прикладное программное обеспечение.

Этот продукт облегчает конечному пользователю решение конкретных задач. Следует, однако, отметить, что грамотный инженерный персонал может и без программистов создать для себя прикладную программу. Для этих целей существуют универсальные инструментальные средства, например электронные таблицы *Excel*. С помощью такого инструмента человек, например экономист, способен создать для себя набор взаимосвязанных таблиц и автоматизировать рутинные, часто повторяющиеся вычислительные операции. Универсальными инструментальными средствами должны обязательно владеть специалисты предприятия.

1.12 Организационно-правовое обеспечение информационных систем

Информация с точки зрения информационной безопасности обладает следующими категориями:

– конфиденциальность, т. е. гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации;

– целостность, т. е. гарантия того, что информация существует в ее исходном виде, т. е. при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения;

– аутентичность, т. е. гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории называется фальсификацией автора сообщения;

– апеллируемость – категория, часто применяемая в электронной коммерции, т. е. гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при фальсификации автора кто-то другой пытается заявить, что он

автор сообщения, а при нарушении апеллируемости – сам автор пытается отказаться от своих слов, подписанных им однажды.

В отношении информационных систем применяются иные категории:

– надежность, т. е. гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано;

– точность, т. е. гарантия точного и полного выполнения всех команд;

– контроль доступа, т. е. гарантия того, что различные группы лиц имеют различный доступ к информационным объектам и эти ограничения доступа постоянно выполняются;

– контролируемость, т. е. гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса;

– контроль идентификации, т. е. гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает;

– устойчивость к умышленным сбоям, т. е. гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

Особенности корпоративной сети обусловливают повышенную опасность этого типа сетей; одной из таких особенностей является наличие глобальных связей, которые простираются на много сотен и тысяч километров, не позволяют воспрепятствовать злонамеренному доступу к передаваемым по этим линиям связи данным. Нельзя дать никаких гарантий, что в некоторой, недоступной для контроля точке пространства, некто не подключится к передающей среде для захвата и последующего декодирования пакетов данных.

К особенностям корпоративной сети относят:

1. Подверженность внешним вторжениям из-за наличия глобальных связей;
2. Масштабность: имеется очень большое количество рабочих станций, серверов, пользователей, мест хранения данных и т. п. В таких условиях администратору оказывается гораздо труднее построить надежную защиту сети, предусматривающую адекватную реакцию на все возможные попытки взлома системы;

3. Гетерогенность – особенность корпоративной сети, которая усложняет работу администратора по обеспечению её безопасности. Действительно, в программно- и аппаратно-неоднородной среде гораздо сложнее проверить согласованность конфигурации разных компонентов и осуществлять централизованное управление. К тому же надо учесть, что в большой гетерогенной сети резко возрастает вероятность ошибок как пользователей, так и администраторов.

По сравнению с сетями масштаба отдела или небольшого предприятия обеспечение безопасности в корпоративной сети является задачей не только более сложной, но и более важной, учитывая материальные потери, к которым может привести доступность некоторых данных для заинтересованных в этом лиц. Это обстоятельство переводит безопасность из разряда чисто технических вопросов в разряд самых приоритетных бизнес-проблем.

Практически любой метод защиты данных основан на том или ином виде шифра. Проблема защиты данных при передаче их через публичные сети осложняется и тем обстоятельством, что во многих странах правительства вводят ограничения на использование основных средств защиты данных, а именно средств их шифрации. Такие ограничения преследуют несколько целей:

– предотвращение утечек государственных секретов, к чему может привести использование в государственных учреждениях непроверенных средств шифрации данных при отправке их в публичные сети (телефонные или компьютерные);

– возможность расшифровки данных, пересылаемых лицами или организациями, подозреваемыми в преступных действиях;

– защита отечественных производителей средств шифрации;

– контроль за рынком средств шифрации.

Повсеместное распространение сетевых продуктов массового потребления, имеющих встроенные средства защиты данных, например, сетевых ОС *Windows* с протоколом защиты данных, с одной стороны, упрощает защиту данных, а с другой – часто создает только видимость надежной защиты.

Кроме надежной шифрации при защите корпоративных данных возникает необходимость в надежной аутентификации пользователей.

Аутентификация – это обеспечение уверенности в том, что данный пользователь является тем индивидуумом, за кого себя выдает. Использование средств удаленного доступа к корпоративной сети существенно усложняет эту задачу. При аутентификации пользователей локальной сети успешно решить ее помогают организационные меры: отсечение посторонних пользователей от клиентских компьютеров и терминалов, контроль за подключениями к кабельной системе здания и т. п. При удаленном доступе эти средства не работают, а пароли, передаваемые легальными пользователями в открытом виде по публичной сети, могут быть перехвачены и использованы впоследствии для нелегальной работы.

Новые проблемы создает проблема аутентификации пользователей при ведении бизнеса через Интернет. Число пользователей вырастает настолько, что количество переходит в качество, и старые методы аутентификации на основе индивидуальных паролей затрудняет работу администратора.

При рассмотрении проблем, связанных с защитой данных в сети, возникает вопрос о классификации сбоев и несанкционированного доступа, что ведет к потере или нежелательному изменению данных. Это могут быть сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и т. д.), потери информации (из-за инфицирования компьютерными вирусами, неправильного хранения архивных данных, нарушений прав доступа к данным), некорректная работа пользователей и обслуживающего персонала.

Перечисленные нарушения работы в сети вызвали необходимость создания различных видов защиты информации. Условно их можно разделить на три класса:

- средства физической защиты;
- программные средства защиты (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);
- административные меры защиты (доступ в помещения, разработка стратегий безопасности фирмы и т. д.).

Одно из средств физической защиты – это системы архивирования и дублирования информации. Наиболее распространенными моделями архивированных серверов являются *Storage Express System* корпорации *Intel*.

Для борьбы с компьютерными вирусами наиболее часто применяются антивирусные программы или аппаратные средства защиты. Однако в последнее время наблюдается тенденция к сочетанию программных и аппаратных методов защиты. Среди аппаратных устройств используются специальные антивирусные платы, вставленные в стандартные слоты расширения компьютера. Кроме антивирусных программ проблема защиты информации в компьютерных сетях решается введением контроля доступа и разграничением полномочий пользователя.

Однако такая система защиты достаточно слаба, так как уровень доступа и возможность входа в систему определяются паролем, который легко подсмотреть или подобрать. Для исключения неавторизованного проникновения в компьютерную сеть используется комбинированный подход с применением пароля и идентификации пользователя по персональному «ключу». «Ключ» представляет собой пластиковую карту (применяется магнитная карта или *smart*-карт со встроенной микросхемой) или различные устройства для идентификации личности по биометрической информации.

По мере расширения деятельности предприятий, роста численности абонентов и появления новых филиалов возникает необходимость организации доступа удаленных пользователей к центральным вычислительным или информационным ресурсам компаний. Для организации удаленного доступа чаще всего используются кабельные линии и радиоканалы. В связи с этим защита информации, передаваемой по каналам удаленного доступа, требует особого подхода. В мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов: их разделение и передача параллельно по двум линиям, что делает невозможным перехват данных при незаконном подключении хакера к одной из линий. Процедура сжатия передаваемых пакетов также гарантирует невозможность расшифровки перехваченных данных.

Мосты и маршрутизаторы удаленного доступа можно запрограммировать таким образом, что удаленным пользователям будут доступны не все ресурсы центра компании.

Наиболее распространенным способом входа в систему при атаках на информацию остается вход через официальную регистрацию системы.

При использовании терминалов с физическим доступом необходимо соблюдать следующие требования:

1. Защищенность терминала должна соответствовать защищенности помещения: терминалы без пароля могут присутствовать только в тех помещениях, куда имеют доступ лица соответствующего или более высокого уровня доступа. Отсутствие имени регистрации возможно лишь в том случае, если к терминалу имеет доступ только один человек, либо если на группу лиц, имеющих к нему доступ, распространяются общие меры ответственности. Терминалы, установленные в публичных местах, должны всегда запрашивать имя регистрации и пароль;

2. Системы контроля за доступом в помещение с установленным терминалом должны работать полноценно и в соответствии с общей схемой доступа к информации;

3. В случае установки терминала в местах с большим скоплением людей клавиатура, а если необходимо, то и дисплей, должны быть оборудованы устройствами, позволяющими видеть их только работающему в данный момент клиенту (непрозрачные стеклянные или пластмассовые ограждения, шторки, «утопленная» модель клавиатуры).

При использовании удаленных терминалов необходимо соблюдать определенные правила, перечисленные далее.

1. Любой удаленный терминал должен запрашивать имя регистрации и пароль.

2. Необходимо своевременное отключение всех модемов, не требующихся в данный момент фирме (например по вечерам или во время обеденного перерыва) либо неконтролируемых в данный момент вашими сотрудниками.

3. По возможности рекомендуется использовать схему возвратного звонка от модема, поскольку она гарантирует с уровнем надежности АТС, то, что удаленный клиент получил доступ с определенного телефонного номера.

4. Из *login*-запроса терминала рекомендуется убрать все непосредственные упоминания имени фирмы, ее логотипы и т. п; – это не позволит компьютерным злоумышленникам, просто перебирающим номера с модемами, узнать, экран регистрации какой фирмы они обнаружили.

5. Также на входе в систему рекомендуется выводить на экран предупреждение о том, что вход в систему без полномочий на это

преследуется по закону. Во-первых, это послужит еще одним предостережением начинающим злоумышленникам, а во-вторых, будет надежным аргументом в пользу атакованной фирмы в судебном разбирательстве, если таковое будет производиться.

Существует два основных метода борьбы с копированием паролей:

– адекватная защита рабочих станций от запуска сторонних программ:

а) отключение сменных носителей информации (гибких дисков);

б) специальные драйверы, блокирующие запуск исполнимых файлов без ведома оператора либо администратора;

в) мониторы, уведомляющие о любых изменениях системных настроек и списка автоматически запускаемых программ;

– система единовременных паролей (при каждой регистрации в системе клиентам с очень высоким уровнем ответственности самой системой генерируется новый пароль).

Сканирование современными антивирусными программами также может помочь в обнаружении «троянских» программ, но только тех из них, которые получили широкое распространение по стране.

Для программного обеспечения бизнес-класса и частной переписки проблему можно решить с помощью криптографии (шифрования). Любой объем информации, будучи зашифрован с помощью достаточно стойкой криптосистемы, недоступен для прочтения без знания ключа.