

NATIONS UNIES

ОБЪЕДИНЕННЫЕ НАЦИИ

UNITED NATIONS

COMMISSION ECONOMIQUE
POUR L'EUROPE
SEMINAIRE

ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ
КОМИССИЯ
СЕМИНАР

ECONOMIC COMMISSION
FOR EUROPE
SEMINAR

СТАТИСТИЧЕСКАЯ КОМИССИЯ И
ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ
КОМИССИЯ



Distr.
GENERAL

КОНФЕРЕНЦИЯ ЕВРОПЕЙСКИХ СТАТИСТИКОВ

CES/SEM.38/38
10 March 1998

RUSSIAN ONLY

Семинар по интегрированнзм статистическим
информационнэм системам и связанным
с ними вопросами (ИСИС-98)
(Братислава, Словацкая Республика,
26-29 мая 1998 года)

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ СВЯЗИ И КОММУНИКАЦИЙ, И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И
КОНФИДЕНЦИАЛЬНОСТИ В РАСПРЕДЕЛЕННЫХ СЕТЯХ СИСТЕМЫ ГОССТАТИСТИКИ СТРАН TACIS

Документ представлен Статистическим управлением Азербайджана¹

1. В современном мире, когда информация во всех сферах жизнедеятельности человечества играет огромную роль, планирование и построение автоматизированных систем обработки и представления информации, учитывая стремительно развивающиеся технологии, является актуальным и ответственным для любого производителя и потребителя информации.
2. Комитеты по статистике стран TACIS вдвойне заинтересованы в этом вопросе, так как одновременно являются потребителями и производителями информации. Учитывая тот факт, что информация комитета статистики охватывает все сферы деятельности общества во всех регионах страны и используется в его регулировании государственными институтами, накладывает особые требования на разработку информационных технологий. В настоящее время в комитетах статистики стран TACIS идет активный переход к современным компьютерным технологиям с использованием локальных сетей объединенных в корпоративной сети статистики с дальнейшим входом в Internet.
3. При преоктировании сетей необходимо учитывать следующие аспекты:
 - (i) соответствие современному мировому уровню развития информационных технологий;

¹ Автор: Джалидов Фанк Али

- (ii) обеспечение надежного высокоскоростного обмена между узлами локальных, корпоративных сетей с регионально распределенными локальными узлами;
- (iii) обеспечение сохранности информации во всех узлах сети и этапах технологического процесса обработки информации;
- (iv) обеспечение надежной защиты информации от несанкционированного доступа (конфиденциальность информации);
- (v) обеспечение возможности модернизации технологического процесса обработки информации без больших затрат с появлением новшеств в информационных технологиях.

4. В данном докладе будут рассмотрены следующие из них:

- a) обеспечение надежного высокоскоростного обмена между узлами локальных, корпоративных сетей с регионально распределенными локальными узлами;
- b) обеспечение сохранности информации во всех узлах сети и этапах технологического процесса обработки информации;
- c) обеспечение надежной защиты информации от несанкционированного доступа.

5. В рамках требований по оформлению доклада невозможно подробно остановиться на всех аспектах указанных проблем, поэтому в данной работе мы постараемся, по возможности кратко, осветить некоторые, на наш взгляд, важные аспекты этих проблем.

Обеспечение надежного высокоскоростного обмена между узлами локальных, корпоративных сетей с регионально распределенными локальными узлами.

6. Успешная работа современных компьютерных сетей во многом зависит от правильно спланированной и реализованной связи между его отдельными элементами. Быстро развивающиеся приложения и технологии требуют значительного увеличения скорости и объема трафика в локальных и глобальных сетях. Уверенность в том, что структурированная кабельная система спроектирована так, что выдержит повышение скорости передачи, связанные с разворачивающимися широкополосными интенсивными приложениями, будет иметь решающее значение.

7. Сегодня средства кабелирования зданий и комплексов включают системы, базирующиеся на оптических, UTP, STP и коаксиальных кабелях. Каждая обеспечивает определённые возможности и имеет преимущества и недостатки и определяется потребностями заказчика.

8. В то время как коаксиальный кабель обеспечивает передачу видеосигналов и низкоскоростную передачу данных, таких как в протоколах Ethernet и IBM 3270, к его недостаткам в кабельных системах относятся размеры, вес, негибкость, трудность прокладки и нехватка поддерживаемых приложений.

9. В свою очередь, STP кабели поддерживают несколько протоколов передачи данных, но их основными недостатками являются трудности прокладки, заземления и стоимость.

10. Среди UTP - кабелей и соединителей к ним имеются две различные, определённые стандартом EIA / TIA-568 категории, между которыми необходимо сделать выбор - Категория 3 и Категория 5 . В то время как Категория 3 обеспечивает передачу голоса и низкоскоростную передачу данных со скоростью до 16 Мбит/с, Категория 5 обеспечивает передачу всех голосовых сигналов данных, в том числе в высокоскоростных локальных сетях, таких как TP - PMD и ATM, с темпом до 155 Мбит/с.

11. Имеется также выбор из двух типов оптических кабелей - с многомодовым и одномодовым волокнами. Исходя из соображений экономической эффективности и совместимости с основанным на оптике сетевым оборудованием, следует выбрать многомодовое волокно. Одномодовое волокно необходимо выбирать для передачи на большие расстояния и когда требуется очень высокая широкополосность.

Комбинация UTP и оптических кабелей.

12. В прошлом медные кабели идеально подходили для низкоскоростных приложений, в то время как оптические кабели были наилучшими для высокоскоростных, удаленных, критических к помехам и требующих секретности. Сегодня высшие показатели кабельной инфраструктуры, базирующихся на медных и оптических кабелях, достигли и превысили пропускную способность в 155 Мбит/с.

13. Для многих пользователей комбинация UTP кабелей Категории 5 и оптических с многомодовым волокном являются наилучшим выбором. Оба кабеля поддерживают широкий набор приложений, специфицированы как средства передачи для появляющихся высокоскоростных локальных сетей и соответствуют практически для всех стандартов проводки.

14. Локальные сети последних нескольких лет , такие как Token Ring и 10 BASE - T/ F, работают в диапазоне от 4 до 16 Мбит/с, тогда как системы, планируемые и развёртываемые в настоящее время, достигли диапазона скоростей до 155 Мбит/с. В будущем скорость передачи может достигнуть до 622 Мбит/с и выше.

15. Даже сегодня специальные приложения, такие как компьютер для массовой памяти и графика высокого разрешения, требуют темпа передачи 1 Гбит/с и выше. Оглядываясь на тенденции роста темпа передачи за последнее десятилетие, легко представить себе потребность в 10 – 100 кратном увеличении темпа передачи, по сравнению с наиболее популярными современными сетями.

16. Уже установлены стандарты, в которых определены возможности повышенного темпа передачи данных. Например – Fiber Channel (Оптический Канал), который определяет возможность передачи данных со скоростью выше чем 1 Гбит/с. Более того, стандарты ATM определяют скорости передачи вплоть до 2,5 Гбит/с.

17. Если требования по скорости передачи в локальных сетях возрастут до уровня, близкого к скорости обработки в компьютере, потребность в инфраструктуре с высокими характеристиками может вскоре появиться на горизонте.

Определение потребности пользователя и выбор.

18. Чтобы определить, какую комбинацию UTP и / или оптических кабелей проложить, каждый заказчик должен установить свою потребность в приложениях, учитывая различные преимущества каждого типа кабеля и их относительную важность. Стоимость, простота прокладки, перемещения и размещения, сегодняшние и ожидаемые в будущем применения, а также ожидаемое время жизни системы – вот типичные главные факторы, влияющие на выбор решения. Соображения, связанные с окружением, такие как электрические помехи и чистота помещений, также могут повлиять на решение, как и тип здания, отрасль промышленности и принадлежность кабельной системы.

19. Потребности в низкоскоростных приложениях, короткое время жизни системы и низкие начальные затраты могут склонить пользователя к выбору системы, содержащей преимущества UTP кабели. Существующие высокоскоростные приложения, жёсткие окружающие условия и приложения с интенсивной графикой мультимедиа могут привести пользователя к выбору системы, базирующейся в основном на оптике. Большинство систем предъявляют требования промежуточные между этими двумя крайностями.

20. Знание того, что имеется некоторое перекрытие в технической базе пользователя и возможностях кабельных систем, основанных на UTP кабелях Категории 5 и оптических многомодовых волокнах, понимание специфических потребностей пользователя необходимы, чтобы рекомендовать оптимальное решение. В пределах бюджетных ограничений, каждый пользователь должен рассмотреть и определить значимость следующих соображений:

- (i) сложность сетевых приложений;
- (ii) вид трафика, ожидаемого в различных частях сети, исходя из числа пользователей, потребностей в передаче данных для каждого пользователя, архитектуры сети и т. д.;
- (iii) ожидаемое время жизни сети и кабельной инфраструктуры;
- (iv) частота перемещений и изменений;
- (v) возможность роста сети сверх ожидаемого времени жизни;
- (vi) неблагоприятные физические условия в сети, такие как жёсткое электромагнитное влияние, радиочастотное влияние, увеличение расстояния или требования повышенного уровня безопасности.

21. Расчитывая экономическую эффективность, следует рассуждать в терминах "стоимость жизненного цикла", а не только начальной стоимости установки. В "стоимости жизненного цикла" учитывается:

- (i) начальная стоимость установки; управление, способность сети к лёгкой и недорогой перестройке;
- (ii) пригодность для будущих применений, способность поддерживать в будущем постоянно растущие ширину полосы и темп передачи;
- (iii) эксплуатация, усилие, требуемые для поддержания работоспособности системы;
- (iv) величина жизненного цикла, обеспечение гарантий, распространяющихся на приложения и оборудование;
- (v) целостность данных, влияние ошибок при передаче данных на работоспособность системы и производительность пользователя.

22. Учитывая особенности системы государственной статистики и территориальную распределенность предполагалось следующая:

- a) Модель учреждений статистики, имеет следующие особенности:
 - (i) она многоузловая (каждое подразделение - это узел);
 - (ii) территориально распределенная - узлы разнесены по регионам страны;
 - (iii) централизованная - система административно управляет из единого центра.
- b) Управление информацией имеет следующие особенности:
 - (i) информация поступает в систему извне (от объектов статистического наблюдения);
 - (ii) информация обрабатывается в каждом узле (проверка, загрузка в базы данных, агрегация, архивирование);
 - (iv) информация представляется заинтересованным организациям и клиентам из любого узла;
 - (v) центральный узел (учреждение статистики страны) имеет доступ к любой информации других узлов.

23. Критерии, которым должна удовлетворять глобальная сеть системы Государственной Статистики страны:

- (i) Сеть должна быть территориально распределенной (Wide-Area Network - WAN) с узлами в региональных подразделениях учреждений статистики.
- (ii) Сеть должна поддерживать новые Internet/Intranet-технологии как для обеспечения управления информацией внутри учреждения, так и для доступа к ней извне.
- (iii) В региональных подразделениях (узлах) должны быть предусмотрены локальные сети, поддерживающие технологию WEB-сервиса.
- (iv) Сетевое оборудование и системное программное обеспечение должны позволять использование для удаленной связи всех видов физических каналов (коммутируемых телефонных каналов, арендованных линий, каналов frame relay, ATM и других).
- (v) Логическая структура и аппаратная конфигурация сети должны быть гибкими, то есть легко адаптироваться к изменениям инфраструктуры учреждения. Они должны предусматривать потенциальный рост конфигурации и добавление новых функциональных возможностей. Они не должны накладывать ограничения на количество клиентов, серверов, логических и физических схем.

24. Учитывая тот факт, что при сравнительно недавнем переходе на компьютерную технологию во всех отраслевых структурах намечается стремительный переход к обработке информации с использованием графических приложений и в дальнейшем возможность использования более современных технологий требующих больших объемов обмена информации и высоких темпов обмена, и надежности, и учитывая запросы не только сегодняшнего дня, а хотя бы на несколько лет вперед, и учитывая ограниченные финансовые возможности для глобальной сети статистики страны может быть предложена следующая структура кабельный системы и связи:

а) Центральный узел (учреждения статистики страны):

- (i) выход в Internet по выделенному каналу и желательно стать провайдером Internet;
- (ii) в глобальной сети, объединяющей все локальные сети центрального аппарата, используется многомодовое волокно;
- (iii) связь с государственными органами управления по выделенным телефонным каналам;
- (iv) в локальных сетях отраслевых управлений УТР Категории 5;
- (v) связь с другими клиентами по выделенным или коммутируемым телефонным линиям;
- (vi) связь с региональными центрами, где имеется локальная сеть по выделенному телефонному каналу;

- (vii) связь с региональными центрами без локальной сети по коммутируемым телефонным каналам.
- b) Региональные узлы (учреждения статистики районного или областного звена где имеется компьютерная сеть):
- (i) выход в Internet по выделенному каналу через центральный узел;
 - (ii) в глобальной сети регионального узла (если таковой имеется) используется многомодовое волокно;
 - (iii) в локальных сетях отраслевых упражлений UTP Категории 5;
 - (iv) связь с отдельными удаленными узлами по коммутируемому телефонному каналу;
 - (v) связь с другими региональными узлами по коммутируемому телефонному каналу.

Безопасность и конфиденциальность информации.

25. Масштабы и сфера применения вычислительной техники в информационных технологиях стали таковы, что наряду с проблемой надежности и устойчивости ее функционирования возникает проблема обеспечения безопасности циркулирующей в ней информации. Безопасность информации - это способность системы ее обработки обеспечить в заданный промежуток времени возможность выполнения заданных требований по величине вероятности наступления событий, выражаяющихся в утечке, модификации или утрате данных, представляющих ту или иную ценность.

26. Причиной таких событий могут быть случайные воздействия или воздействия в результате преднамеренного несанкционированного доступа.

27. В результате утечки информации могут раскрываться какие либо тайны: государственной, военной, служебной, коммерческой или личной.

28. Защищенные должны подлежать не только секретная информация, а также служебная или другая информация, модификация которой может привести к утечке секретной информации или получению пользователем ложной информации.

29. Разрушение или исчезновение данных может привести к их невосполнимой утрате.

30. Учитывая сказанное все потенциальные угрозы могут быть сведены к следующим трем : утечка, модификация и утрата.

31. С переходом на использование технических средств связи информация подвергается воздействию случайных процессов: неисправностям, сбоям оборудования, ошибкам производителя или пользователя и т.д., которые могут

привести к утечке, модификации (изменения на ложную), утрате или доступу к ним посторонних лиц. Появление персональных компьютеров, использование локальных и глобальных сетей, подключением к Internet и использованием технологий клиент сеть и активных сетей расширяются возможности не только пользователей, но и нарушителей, таких как хакеры, крэкеры и компьютерные вирусы.

32. С входом в Internet и использованием активных сетей угроза воздействия со стороны компьютерных вирусов становится все более ощутимой и борьба с ними и ликвидация последствий их действий требуют больших усилий и материальных затрат, и поэтому, изучению их и борьбе с ними надо уделять особое внимание.

33. Компьютерные вирусы также можно разделить на следующие категории:

- (i) вирусы создающие помеху в виде безобидных шуток или юмористических помех;
- (ii) вирусы задерживающие выполнение работ;
- (iii) вирусы разрушающие информацию и программное обеспечение пользователя;
- (iv) вирусы разрушающие вычислительную технику;
- (v) вирусы разведчики.

Потенциальные угрозы безопасности информации в компьютерных сетях.

34. Исследования и анализ многочисленных случаев воздействия на информацию и несанкционированного доступа к ней показывает, что их можно разделить на случайные и преднамеренные.

Последствия, к которым приводит реализация угроз: разрушение информации, модификация и ознакомление с ней посторонних лиц. Цены указанных событий могут быть самыми различными: от недоразумений до катастрофических последствий для определенной группы людей или общества.

Предупреждение приведенных последствий в автоматизированных системах обработки информации и является целью создания системы безопасности информации.

35. Причинами случайных угроз для информации на компьютерных сетях могут быть:

- (i) отказы и сбои аппаратуры;
- (ii) помехи на линиях связи от воздействия внешней среды;
- (iii) ошибки человека как звена системы;
- (iv) схемные и системотехнические ошибки разработчиков;
- (v) структурные, алгоритмические и программные ошибки;
- (vi) аварийные ситуации и другие воздействия.

36. Причины для преднамеренных угроз могут быть самыми различными- начиная от простой обиды, кончая просто сумасшествием.

Современные методы защиты информации в компьютерных сетях.

37. С использованием современных компьютерных технологий, усложнением обработки, увеличением количества технических средств увеличивается количество и виды случайных воздействий на информацию, а также возможные каналы несанкционированного доступа к ней. С увеличением объема, сосредоточением информации, увеличением количества пользователей и другими указанными выше причинами, увеличивается вероятность преднамеренного несанкционированного доступа к информации. В связи с указанными причинами развиваются старые и возникает новые методы защиты информации в компьютерных сетях:

- (i) методы функционального контроля, обеспечивающие обнаружение и диагностику отказов, сбоев аппаратуры и ошибок человека, а также программные ошибки;
- (ii) методы повышения достоверности информации;
- (iii) методы защиты информации от аварийных ситуаций;
- (iv) методы контроля доступа к внутреннему монтажу аппаратуры, линиям связи и технологическим органам управления;
- (v) методы разграничения и контроля доступа к информации;
- (vi) методы идентификации и аутентификации пользователей, технических средств, носителей информации и документов;
- (vii) методы защиты от побочного излучения и наводок информации.

Ограничение доступа.

38. Ограничение доступа заключается в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.

39. Ограничение доступа к комплексам средств автоматизации обработки информации заключается:

- (i) в выделении специальной территории для размещения комплексов средств автоматизации;
- (ii) в сооружении по периметру зоны специальных ограждений с охранной сигнализацией;
- (iii) в сооружении специальных зданий или других сооружений;
- (iv) выделение специальных помещений в здании;
- (v) в создании контрольно-пропускного режима на территории, в зданиях и помещениях.

Контроль доступа к аппаратуре.

40. С позиций защиты информации от несанкционированного доступа контроль вскрытия аппаратуры защищает от следующих действий :

- (i) изменения и разрушения принципиальной схемы вычислительной системы и аппаратуры;
- (ii) подключения постороннего устройства;
- (iii) изменение алгоритма работы вычислительной системы путём использования технологических пультов и органов управления;
- (iv) загрузки посторонних программ и внесения программных "вирусов" в систему;
- (v) использование терминалов посторонними лицами и т. д.

Разграничение и контроль доступа к информации.

41. Разграничение доступа в вычислительной системе заключается в разделении информации, циркулирующей в ней, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

41. Задача разграничения доступа : сокращение количества должностных лиц, не имеющих к ней отношения при выполнении своих функций, т. е. защита информации от нарушителя среди допущенного к ней персонала .

42. При этом деление информации может производиться по степени важности, секретности , по функциональному назначению, по документам и т. д.

43. Принимая во внимание, что доступ осуществляется с различных средств, начать разграничение можно путём разграничения доступа к техническим средствам, разместив их в отдельных помещениях. Все подготовительные функции технического обслуживания аппаратуры, её ремонта, профилактики, перезагрузки программного обеспечения и т. д. должны быть технически и организационно отделены от основных задач системы.

Криптографическое преобразование информации.

44. Защита информации методом криптографического преобразования заключается в преобразовании ее составных частей с помощью специальных алгоритмов либо аппаратных решений и кодов ключей. Использование криптографии является одним из распространенных методов, значительно повышающих безопасность передачи данных в сетях, данных хранящихся в удаленных устройствах памяти, и при обмене информацией между удаленными объектами.

45. Множество современных методов защитных преобразований можно классифицировать на четыре большие группы: перестановки, замены(подстановки), аддитивные и комбинированные методы.
Методы подстановки и перестановки обычно характеризуются короткой длиной ключа, а надежность их защиты определяется сложностью алгоритмов преобразования.

46. Для аддитивных методов характерны простые алгоритмы преобразования, их надежность основана на увеличении длины ключа.
Все перечисленные методы относятся к симметричному шифрованию: один и тот же ключ используется для шифрования и дешифрования.

Методы и средства защиты информации от случайных воздействий.

47. Проблема надежности автоинтилизированных систем решается тремя способами:
(i) повышением надежности деталей и узлов;
(ii) построением надежных систем из менее надежных узлов за счет структурной избыточности (дублирование, утройство элементов, устройств и подсистем и т.д.)
(iii) применения функционального контроля с диагностикой отказа, увеличивающего надежность функционирования системы, путем сокращения времени восстановления отказавшей аппаратуры.

Обеспечение надежной защиты информации от несанкционированного доступа.

48. Предметом защиты в автоматизированных системах обработки информации являются данные, циркулирующие и хранимые в виде команд, сообщений и т.д., представляющие какую-либо ценность для их владельца и потенциального нарушителя. При этом, за несанкционированный доступ принимаем событие, выражющиеся в попытке нарушителя совершить несанкционированное действие по отношению любой ее части.

49. К каналам, по которым могут быть осуществлены несанкционированные доступы к информации , в вычислительной сети можно пречислить:

- (i) терминалы пользователей;
- (ii) средства отображения и документирования информации;
- (iii) средства загрузки программного обеспечения в систему;
- (iv) любые носители информации;
- (v) внешние каналы связи;
- (vi) технологические пульты и органы управления;
- (vii) внутренний монтаж аппаратуры;
- (viii) побочное электромагнитное излучение и т.д.

50. Опасность преднамеренных несанкционированных действий заключается во вводе нарушителем незаконных команд, запросов, сообщений, программ и т.д., приводящих к утрате, модификации информации и несанкционированного ознакомления с нею, а также перехвате нарушителем информации путем приема и наблюдения сигналов побочного электромагнитного излучения и наводок.

51. Возможные каналы несанкционированного доступа можно разделить на две категории: контролируемые и неконтролируемые.

52. К контролируемым каналам можно отнести:

- (i) терминалы пользователей;
- (ii) средства отображения и документирования информации;
- (iii) средства загрузки программного обеспечения в систему;
- (iv) внутренний монтаж аппаратуры;
- (v) побочное электромагнитное излучение.

53. К неконтролируемым каналам можно отнести:

- (i) любые носители информации, выносимые за пределы вычислительной системы;
- (ii) внешние каналы связи.

54. Поскольку физические каналы связи в сети защитить не представляется возможным, целесообразно строить защиту информации и сопровождающих ее служебных признаков на основе специальных криптографических преобразований. Такой основой должна быть кодограмма сообщений, которой обмениваются между собой клиенты сети. Целостность этой кодограммы и содержащаяся в ней информация должны быть защищены от несанкционированного доступа.

55. Для того, чтобы обеспечить возможность контроля и разграничения доступа, необходимо для всех участников обмена информацией, помимо условных номеров, присвоить переменные идентификаторы в виде паролей, которые могут передаваться в открытом виде и подлинность которого будет обеспечиваться механизмом цифровой подписи. Тем абонентам, которым присвоены соответствующие полномочия, должны быть представлены соответствующие значения паролей и закрытых ключей шифрования.

Защита от преднамеренного несанкционированного доступа.

56. Анализ локальных сетей как объекта защиты, возможных каналов несанкционированного доступа к информации ограниченного пользования и потенциальных угроз позволяет выбрать и построить соответствующую систему защиты.

57. Перечисленные выше возможные каналы несанкционированного доступа рассмотрены с позиций максимально возможных угроз, ожидаемых от нарушителя – профессионала, модель поведения которого, как наиболее опасная, принята за исходную предпосылку в концепции защиты. Поэтому, несмотря на существующие на практике менее опасные модели, будем пока следовать принятым ранее решениям.

58. Несанкционированный доступ со стороны пользователя – нарушителя, очевидно, потребуют создания, на программном уровне, локальных сетей системы опознания и разграничения доступа к информации со всеми её атрибутами : средствами идентификации и аутентификации пользователей, а также разграничения их полномочий по доступу к информации файл-сервера и (или) другим ПК данной локальной сети. Такими возможностями, например, обладает система NetWare.

59. Средства защиты сети NetWare позволяет устанавливать, кто имеет право доступа к конкретным каталогам и файлам. При этом защита данных файл-сервера осуществляется одним способом или, в различных сочетаниях, четырьмя способами:

- (i) входным паролем;
- (ii) попечительской защитой данных;
- (iii) защитой в каталоге;
- (iv) защитой атрибутами файлов.

60. Первым уровнем сетевой защиты является защита данных входным паролем. Защита при входе в сеть применяется по отношению ко всем пользователям. Чтобы войти в файл-сервер, пользователю нужно знать своё "имя" и соответствующий пароль (6-8 символов).

61. Администратор сети может установить дополнительные ограничения по входу в сеть:

- (i) ограничить период времени, в течение которого пользователь может входить в сеть;
- (ii) назначить рабочим станциям специальные адреса, с которыми разрешено входить в сеть;
- (iii) ограничить количество рабочих станций, с которых можно войти в сеть;
- (iv) установить режим "запрета постороннего вторжения", когда при нескольких несанкционированных попытках с неверным паролем, устанавливается запрет на вход в сеть.

62. Второй уровень защиты данных в сети – попечительская защита данных – используется для управления возможностями индивидуальных пользователей по работе с файлами в заданном каталоге. Попечитель – это пользователь, которому предоставлены привилегии или права для работы с каталогом и файлами внутри него.

63. Любой попечитель может иметь восемь разновидностей прав :

- (i) Read - право Чтения открытых файлов;
- (ii) Write - право Записи в открытые файлы;
- (iii) Open - право Открытия существующего файла;
- (iv) Create - право Создания (и одновременного открытия) новых файлов;
- (v) Delete - право Удаления существующих файлов;
- (vi) Parental - Родительские права (право Создания, Переименования, Стирания подкаталогов каталога; право Установления попечителей и прав в каталоге; право Установления попечителей и прав в подкаталоге)
- (vii) Search - право Поиска каталога;
- (viii) Modify - право Модификации файловых атрибутов.

64. Третий уровень защиты данных в сети NetWare - защита данных в каталоге. Каждый каталог имеет "маску максимальных прав". Когда создаётся каталог, маска прав содержит также восемь разновидностей прав, что и попечитель. Ограничения каталога применяются только в одном заданном каталоге. Защита в каталоге не распространяется на его подкаталоги.

65. Защита атрибутами файлов - четвёртый уровень защиты данных в сети. При этом предусмотрена возможность устанавливать, может ли индивидуальный файл быть изменён или разделен. Защита атрибутами файлов используется в основном для предотвращения случайных изменений или удаления отдельных файлов. Такая защита, в частности, полезна для защиты информационных файлов общего пользования, которые обычно читаются многими пользователями. Эти файлы не должны допускать порчи при попытках изменений или стирания. В защите данных используются четыре файловых атрибута : "Запись- чтение/ Только чтение" и "Разделяемый / Неразделяемый".

66. Действующие права в сети NetWare - это права, которые пользователь может применять в данном каталоге. Действующие права определяются сочетанием прав попечительской защиты и прав защиты в каталогах. Файловые атрибуты имеют приоритет над действующими правами пользователя. Однако средства защиты информации в сети NetWare не всегда удовлетворяют требованиям всех потребителей. Поэтому есть необходимость разработок дополнительных систем и комплексов защиты.

67. Чтобы исключить возможность обхода систем опознания и разграничения доступа в ПК и локальных сетей путём применения отладочных программ, а также проникновения компьютерных вирусов, рекомендуется, если это возможно, в данной локальной сети применять ПК без дисководов или по крайней мере хотя бы заблокировать их механической крышкой, опечатываемой администратором

безопасности. Данная мера, кроме того, защищает от кражи данных, которые можно скопировать на флоппи диски в течение нескольких минут. Диски легко спрятать и вынести за пределы даже охраняемой территории. Многие поставщики сетей сейчас обеспечивают возможность загрузки локальных рабочих станций с центрального сервера и таким образом делают ПК без диска пригодной для использования в сети.
