# Оглавление

# ВВЕДЕНИЕ

В данном дипломном проекте рассматривается проблема построения локальной вычислительной сети подразделения организации под управлением операционной системы Windows NT.

Реализация предложенного проекта позволит сократить бумажный документооборот внутри подразделения, повысить производительность труда, сократить время на обработку информации.

Но объединение компьютеров в локальную вычислительную сеть привносит и новые трудности. Так как подразделение ведет работу с закрытой информацией, доступ к которой посторонним лицам строго запрещен, то возникает проблема защиты информации в ЛВС.

Локальная вычислительная сеть должна быть спроектирована таким образом, чтобы обеспечить надлежащую степень защищенности данных. Надо помнить, что от этого не должно страдать удобство пользователей и администраторов сети.

ЛВС подразделения управляется операционной системой Windows NT. Предполагается провести исследование встроенных возможностей этой ОС по защите информации от несанкционированного доступа. На основе проведенного анализа сделать выводы и выбрать дополнительные средства, повышающие степень защиты данных.

# 1.ФУНКЦИОНАЛЬНАЯ СХЕМА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

## 1.1.Организационно-штатная структура подразделения

Рассмотрим организационно-штатную структуру подразделения.

Во главе подразделения стоит начальник подразделения.

В состав подразделения входят 3 отделения, а также специализированный отдел прямого подчинения начальнику.

Каждое отделение делится на 2 отдела.

Каждый отдел, в свою очередь разделяется на 3 сектора.

Все вышесказанное иллюстрирует рис.1.1.

Всего в подразделении задействовано 60 человек, которым предполагается выделить в пользование персональный компьютер.

6-ой отдел

5-ый отдел

3-ий отдел

2-ой отдел

20 сектор

19 сектор

7-ой

отдел

1-ый отдел

Отдел прямого подчинения

3-е отделение

2-ое отделение

1-ое отделение

Начальник подразделения

21 сектор

4-ый отдел

16 сектор

13 сектор

10 сектор

7 сектор

4 сектор

1 сектор

17 сектор

14 сектор

11 сектор

8 сектор

5 сектор

2 сектор

18 сектор

15 сектор

12 сектор

9 сектор

6 сектор

3 сектор

Рис.1.1.Организационная структура подразделения.

## 1.2.Информационные потоки в сети подразделения

На рис.1.2 представлена схема информационных потоков в рассматриваемом подразделении.

Рис.1.2. Схема информационных потоков ЛВС

Наиболее подробно показаны информационные потоки в пределах одного сектора (для примера взят 1-ый сектор). В других секторах картина потоков информации аналогична.

## 1.3.Логическая организация сетей Windows NT

### 1.3.1.Понятие домена и связи доверия

Основным элементом централизованного администрирования в Windows NT Server является *домен*. Домен - это группа серверов, работающих под управлением Windows NT Server, которая функционирует, как одна система. Все серверы Windows NT в домене используют один и тот же набор учетных карточек пользователя, поэтому достаточно заполнить учетную карточку пользователя только на одном сервере домена, чтобы она распознавалась всеми серверами этого домена.

*Связи доверия* - это связи между доменами, которые допускают *сквозную идентификацию*, при которой пользователь, имеющий единственную учетную карточку в домене, получает доступ к целой сети. Если домены и связи доверия хорошо спланированы, то все компьютеры Windows NT распознают каждую учетную карточку пользователя и пользователю надо будет ввести пароль для входа в систему только один раз, чтобы потом иметь доступ к любому серверу сети[1].

### 1.3.2.Домены: основные административные блоки

Группирование компьютеров в домены дает два важных преимущества сетевым администраторам и пользователям. Наиболее важное - серверы домена составляют (формируют) единый административный блок, совместно использующий службу безопасности и информацию учетных карточек пользователя. Каждый домен имеет одну базу данных, содержащую учетные карточки пользователя и групп, а также установочные параметры политики безопасности. Все серверы домена функционируют либо как первичный контроллер домена, либо как резервный контроллер домена, содержащий копию этой базы данных. Это означает, что администраторам нужно управлять только одной учетной карточкой для каждого пользователя, и каждый пользователь должен использовать (и помнить) пароль только одной учетной карточки. Расширяя административный блок с единственного компьютера на целый домен, Windows NT Server сохраняет усилия администраторов и время пользователей.

Второе преимущество доменов сделано для удобства пользователей: когда пользователи просматривают сеть в поисках доступных ресурсов, они видят сеть, сгруппированную в домены, а не разбросанные по всей сети серверы и принтеры[1].

### 1.3.3.Связи доверия

Устанавливая связь доверия между доменами сети, мы позволяем использовать учетные карточки пользователя и глобальных групп одного домена в других доменах. Домен облегчает администрирование, поскольку нужно создать учетную карточку для каждого пользователя только один раз, и она даст ему доступ к любому компьютеру сети, а не только к компьютерам одного домена.

Когда устанавливаются отношения доверия между доменами, один домен (доверяющий домен) доверяет другому домену (домен, которому доверяют или доверенный домен).

Согласно этому, доверяющий домен распознает всех пользователей и глобальные группы, учтенные в домене, которому доверяют. Эти учетные карточки могут быть по-разному использованы в доверяющем домене; они могут начать сеанс на рабочих станциях доверяющего домена, могут быть добавлены к локальной группе доверяющего домена и им могут быть даны разрешения и права доверяющего домена.

Отношение (связь) доверия может быть односторонним или двухсторонним. Двухстороннее отношение (связь) доверия - просто пара односторонних связей, где каждый домен доверяет другому.

Доверие между доменами не наследуется. Например, если А доверяет В, а В доверяет С, А автоматически не доверяет С. Чтобы А доверял С (и таким образом можно было бы использовать учетные карточки С в домене А), необходимо установить дополнительное отношение доверия непосредственно между этими доменами[1](рис.1.3).

Домен С

Домен В

Домен А

Рис.1.3. Наследование связей доверия.

### 1.3.4.Требования к домену

Минимальное требование для домена - один сервер, работающий под управлением Windows NT Server, который служит в качестве *первичного контроллера домена* и хранит оригинал базы данных учетных карточек пользователя и групп домена. В дополнение к сказанному, домен может также иметь другие серверы, работающие под управлением Windows NT Server и служащие в качестве *резервных контроллеров домена*, а также компьютеры, служащие в качестве стандартных серверов, серверов LAN Manager 2.x, клиентов Windows NT Workstation и других клиентов, как например, работающих с MS-DOS(рис.1.4).

Рис.1.4. Структура домена.

Первичный контроллер домена должен быть сервером, работающим по управлением Windows NT Server. Все изменения базы данных, учетных карточек пользователя и групп домена должны выполняться в базе данных первичного контроллера домена.

Резервные контроллеры домена, работающие под управлением Windows NT Server, хранят копию базы данных учетных карточек домена. База данных учетных карточек копируется во все резервные контроллеры домена.

Все резервные контроллеры домена дополняют первичный контроллер и могут обрабатывать запросы на начала сеанса от пользователей учетных карточек домена. Если домен получает запрос на начало сеанса, первичный контроллер домена или любой из резервных контроллеров домена может идентифицировать попытку начала сеанса.

Дополнительно к первичным и резервным контроллерам домена, работающим под управлением Windows NT Server, есть другой тип серверов. Во время установки Windows NT они определяются, как “серверы”, а не контроллеры домена. Сервер, который входит в домен, не получает копию базы данных пользователей домена[1].

### 1.3.5.Модели домена

Очень важным моментом является планировка домена.

Есть четыре модели для организации сети: *модель единственного домена, модель основного домена, модель многочисленных основных доменов и модель полного доверия*.

## 1.4.Выбор модели домена

### 1.4.1.Модель единственного домена

Если сеть имеет не слишком много пользователей и не должна делиться по организационным причинам, можно использовать самую простую модель - модель единственного домена. В этой модели сеть имеет только один домен. Естественно, все пользователи регистрируются в этом домене.

Никаких связей доверия не нужно, поскольку в сети существует только один домен.

Чтобы гарантировать хорошую производительность сети, можно использовать модель единственного домена, при условии, что у нее небольшое количество пользователей и групп. Точное количество пользователей и групп зависит от количества серверов в домене и аппаратных средств серверов[1].

### 1.4.2.Модель основного домена

Для предприятий, где сеть имеет небольшое количество пользователей и групп, но должна быть разделена на домены из организационных соображений, основная модель домена может быть наилучшим выбором. Эта модель дает централизованное управление и организационные преимущества управления многими доменами.

В этой модели один домен - основной домен, в котором регистрируются все пользователи и глобальные группы. Все другие домены сети доверяют этому домену и таким образом можно использовать пользователей и глобальные группы, зарегистрированные в них.

Основная цель главного домена - управление сетевыми учетными карточками пользователя. Другие домены в сети - домены ресурса; они не хранят учетные карточки пользователя и не управляют ими, а только обеспечивают ресурсы (как например, файлы и принтеры коллективного использования) сети.

В этой модели только первичные и резервные контроллеры домена в основном домене имеют копии учетных карточек пользователей сети[1].

### 1.4.3.Модель многочисленных основных доменов

Для больших предприятий, которые хотят иметь централизованную администрацию, модель многочисленных основных доменов может оказаться наилучшим выбором, поскольку он наиболее масштабируемый.

В этой модели небольшое количество основных доменов. Основные домены служат в качестве учетных доменов и каждая учетная карточка пользователя создается в одном из этих основных доменов.

Каждый основной домен доверяет всем другим основным доменам. Каждый ведомственный домен доверяет всем основным доменам, но ведомственным доменам не нужно доверять друг другу[1].

### 1.4.4.Модель полного доверия

При желании управлять пользователями и доменами, распределенными среди различных отделов, децентрализовано, можно использовать модель полного доверия. В ней каждый домен сети доверяет другому домену. Таким способом каждый отдел управляет своим собственным доменом и определяет своих собственных пользователей и глобальные группы, и эти пользователи и глобальные группы могут, тем не менее, использоваться во всех других доменах сети.

Из-за количества связей доверия, необходимого для этой модели, она не практична для больших предприятий[1].

### 1.4.5.Выбор модели организации сети

Проанализировав оргонизационно-штатную структуру подразделения, можно заключить, что оптимальным выбором является модель основного домена. Ее достоинства и недостатки сведены в табл.1.1.

Таблица 1.1

Преимущества и недостатки модели основного домена.

|  |  |
| --- | --- |
| **Преимущества** | Недостатки |
| Учетные карточки пользователей могут управляться централизовано. | Ухудшение производительности в случае, если домен будет дополнен большим числом пользователей и групп. |
| Ресурсы сгруппированы логически. | Локальные группы должны быть определены в каждом домене, где они будут использоваться. |

Таблица 1.1(продолжение)

|  |  |
| --- | --- |
| **Преимущества** | Недостатки |
| Домены отделений могут иметь своих собственных администраторов, которые управляют ресурсами в отделе. |  |
| Глобальные группы должны быть определены только один раз (в основном домене). |  |

Логическая структура сети показана на рис.1.5.

* Все пользователи
* Глобальные группы
* Локальные группы

**Основной**

**домен**

**Отдел прямого подчинения**

**1-ое отделение**

**3-е отделение**

**2-ое отделение**

* Локальные группы
* Локальные группы
* Локальные группы

Рис.1.5. Логическая структура сети.

Функциональная схема подразделения, разработанная с учетом всего вышесказанного, приведена на рис.1.6.

Рис.1.6. Функциональная схема ЛВС подразделения

# 2.СТРУКТУРНАЯ СХЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ЛВС

## 2.1.Потенциальные угрозы безопасности информации

Исследование и анализ многочисленных случаев воздействий на информацию и несанкционированного доступа к ней показывают, что их можно разделить на случайные и преднамеренные.

Для создания средств защиты информации необходимо определить природу угроз, формы и пути их возможного проявления и осуществления в автоматизированной системе. Для решения поставленной задачи все многообразие угроз и путей их воздействия приведем к простейшим видам и формам, которые были бы адекватны их множеству в автоматизированной системе.

### 2.1.1.Случайные угрозы

Исследование опыта проектирования, изготовления, испытаний и эксплуатации автоматизированных систем говорят о том, что информация в процессе ввода, хранения , обработки, ввода и передачи подвергается различным случайным воздействиям.

Причинами таких воздействий могут быть:

* Отказы и сбои аппаратуры
* Помехи на линии связи от воздействий внешней среды
* Ошибки человека как звена системы
* Системные и системотехнические ошибки разработчиков
* Структурные, алгоритмические и программные ошибки
* Аварийные ситуации
* Другие воздействия.

Частота отказов и сбоев аппаратуры увеличивается при выборе и проектировании системы, слабой в отношении надежности функционирования аппаратуры. Помехи на линии связи зависят от правильности выбора места размещения технических средств АСУ относительно друг друга и по отношению к аппаратуре соседних систем.

К ошибкам человека как звена системы следует относить ошибки человека как источника информации, человека-оператора, неправильные действия обслуживающего персонала и ошибки человека как звена, принимающего решения.

Ошибки человека могут подразделяться на *логические* (неправильно принятые решения), *сенсорные* (неправильное восприятие оператором информации) и *оперативные*, или *моторные* (неправильная реализация решения). Интенсивность ошибок человека может колебаться в широких пределах: от 1-2% до 15-40% и выше общего числа операций при решениях задачи.

К угрозам случайного характера следует отнести аварийные ситуации, которые могут возникнуть на объекте размещения автоматизированной системы. К аварийным ситуациям относятся:

* Отказ от функционирования САУ в целом, например выход из строя электропитания
* Стихийные бедствия: пожар, наводнение, землетрясение, ураганы, удары молнии и т.д.

Вероятность этих событий связана прежде всего с правильным выбором места размещения АСУ, включая географическое положение[2].

### 2.1.2.Преднамеренные угрозы

Преднамеренные угрозы связаны с действиями человека, причинами которых могут быть определенное недовольство своей жизненной ситуацией, сугубо материальный интерес или простое развлечение с самоутверждением своих способностей, как у хакеров, и т.д.

Для вычислительных систем характерны следующие штатные каналы доступа к информации:

* Терминалы пользователей
* Терминал администратора системы
* Терминал оператора функционального контроля
* Средства отображения информации
* Средства загрузки программного обеспечения
* Средства документирования информации
* Носители информации
* Внешние каналы связи.

Имея в виду, что при отсутствии защиты нарушитель может воспользоваться как штатными, так и другими физическими каналами доступа, назовем возможные каналы несанкционированного доступа (ВКНСД) в вычислительной системе, через которые возможно получить доступ к аппаратуре, ПО и осуществить хищение, разрушение, модификацию информации и ознакомление с нею:

* Все перечисленные штатные средства при их использовании законными пользователями не по назначению и за пределами своих полномочий
* Все перечисленные штатные средства при их использовании посторонними лицами
* Технологические пульты управления
* Внутренний монтаж аппаратуры
* Линии связи между аппаратными средствами данной вычислительной системы
* Побочное электромагнитное излучение аппаратуры системы
* Побочные наводки по сети электропитания и заземления аппаратуры
* Побочные наводки на вспомогательных и посторонних коммуникациях
* Отходы обработки информации в виде бумажных и магнитных носителей.

Очевидно, что при отсутствии законного пользователя, контроля и разграничения доступа к терминалу квалифицированный нарушитель легко воспользуется его функциональными возможностями для несанкционированного доступа к информации путем ввода соответствующих запросов и команд. При наличии свободного доступа в помещение можно визуально наблюдать информацию на средствах отображения и документирования, а на последних похитить бумажный носитель, снять лишнюю копию, а также похитить другие носители с информацией: листинги, магнитные ленты, диски и т.д.

Особую опасность представляет собой бесконтрольная загрузка программного обеспечения в ЭВМ, в которой могут быть изменены данные, алгоритмы или введена программа “*троянский конь*”, выполняющая дополнительные незаконные действия: запись информации на посторонний носитель, передачу в каналы связи другого абонента вычислительной сети, внесение в систему компьютерного вируса и т.д.

Опасной является ситуация, когда нарушителем является пользователь системы, который по своим функциональным обязанностям имеет законный доступ к одной части информации, а обращается к другой за пределами своих полномочий.

Со стороны законного пользователя существует много способов нарушить работу вычислительной системы, злоупотреблять ею, извлекать, модифицировать или уничтожать информацию. Свободный доступ позволит ему обращаться к чужим файлам и банкам данных и изменять их случайно или преднамеренно.

При техническом обслуживании (профилактике и ремонте) аппаратуры могут быть обнаружены остатки информации на магнитной ленте, поверхностях дисков и других носителях информации. Обычное стирание информации не всегда эффективно. Ее остатки могут быть легко прочитаны. При транспортировке носителя по неохраняемой территории существует опасность его перехвата и последующего ознакомления посторонних лиц с секретной информацией.

Не имеет смысла создание системы контроля и разграничения доступа к информации на программном уровне, если не контролируется доступ к пульту управления ЭВМ, внутреннему монтажу аппаратуры, кабельным соединениям.

Срабатывание логических элементов обусловлено высокочастотным изменением уровней напряжений и токов, что приводит к возникновению в эфире, цепях питания и заземления, а также в параллельно расположенных цепях и индуктивностях посторонней аппаратуры, электромагнитных полей и наводок, несущих в амплитуде, фазе и частоте своих колебаний признаки обрабатываемой информации. С уменьшением расстояния между приемником нарушителя и аппаратными средствами вероятность приема сигналов такого рода увеличивается.

Непосредственное подключение нарушителем приемной аппаратуры и специальных датчиков к цепям электропитания и заземления, к каналам связи также позволяет совершить несанкционированное ознакомление с информацией, а несанкционированное подключение к каналам связи передающей аппаратуры может привести и к модификации информации[2].

За последнее время в разных странах проведено большое количество исследовательских работ с целью обнаружения потенциальных каналов несанкционированного доступа к информации в вычислительных сетях. При этом рассматриваются не только возможности нарушителя, получившего законный доступ к сетевому оборудованию, но и воздействия, обусловленные ошибками программного обеспечения или свойствами используемых сетевых протоколов. Несмотря на то, что изучение каналов НСД продолжается до сих пор, уже в начале 80-ых годов были сформулированы пять основных категорий угроз безопасности данных в вычислительных сетях:

1. Раскрытие содержания передаваемых сообщений
2. Анализ трафика, позволяющий определить принадлежность отправителя и получателя данных к одной из групп пользователей сети, связанных общей задачей
3. Изменение потока сообщений, что может привести к нарушению режима работы какого-либо объекта, управляемого из удаленной ЭВМ
4. Неправомерный отказ в предоставлении услуг
5. Несанкционированное установление соединения.

Угрозы 1 и 2 можно отнести к утечке информации, угрозы 3 и 5 – к ее модификации, а угрозу 4 – к нарушению процесса обмена информацией[2].

## 2.2.Средства защиты информации в ЛВС

Принято различать пять основных средств защиты информации:

* Технические,
* Программные,
* Криптографические,
* Организационные,
* Законодательные.

Рассмотрим эти средства подробнее и оценим их возможности в плане дальнейшего их использования при проектировании конкретных средств защиты информации в ЛВС.

### 2.2.1.Технические средства защиты информации

*Технические средства защиты* – это механические, электромеханические, оптические, радио, радиолокационные, электронные и другие устройства и системы, способные выполнять самостоятельно или в комплексе с другими средствами функции защиты данных.

Технические средства защиты делятся на *физические* и *аппаратные*. К физическим средствам относятся замки, решетки, охранные сигнализации, оборудование КПП и др.; к аппаратным – замки, блокировки и системы сигнализации о вскрытии, которые применяются на средствах вычислительной техники и передачи данных.

### 2.2.2.Программные средства защиты информации

*Программные средства защиты* – это специальные программы, включаемые в состав программного обеспечения системы, для обеспечения самостоятельно или в комплексе с другими средствами, функций защиты данных.

По функциональному назначению программные средства можно разделить на следующие группы:

1. *Программные средства идентификации и аутентификации пользователей.*

Идентификация – это присвоение какому-либо объекту или субъекту уникального образа, имени или числа. Установление подлинности (аутентификация) заключается в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

Конечная цель идентификации и установления подлинности объекта в вычислительной системе – допуск его к информации ограниченного пользования в случае положительного результата проверки или отказ в допуске в противном случае.

Одним из распространенных методов аутентификации является присвоение лицу уникального имени или числа – пароля и хранение его значения в вычислительной системе. При входе в систему пользователь вводит свой код пароля, вычислительная система сравнивает его значение со значением, хранящимся в своей памяти, и при совпадении кодов открывает доступ к разрешенной функциональной задаче, а при несовпадении – отказывает в нем.

Наиболее высокий уровень безопасности входа в систему достигается разделением кода пароля на две части, одну, запоминаемую пользователем и вводимую вручную, и вторую, размещаемую на специальном носителе – карточке, устанавливаемой пользователем на специальное считывающее устройство, связанное с терминалом.

1. *Средства идентификации и установления подлинности технических средств.*

Дополнительный уровень защиты по отношению к паролям пользователей.

В ЭВМ хранится список паролей и другая информация о пользователях, которым разрешено пользоваться определенными терминалами, а также таблица ресурсов, доступных с определенного терминала конкретному пользователю.

1. *Средства обеспечения защиты файлов.*

Вся информация в системе, хранимая в виде файлов делится на некоторое количество категорий по различным признакам, выбор которых зависит от функций, выполняемых системой. Наиболее часто можно встретить разделение информации:

* по степени важности
* по степени секретности
* по выполняемым функциям пользователей
* по наименованию документов
* по видам документов
* по видам данных
* по наименованию томов, файлов, массивов, записей
* по имени пользователя
* по функциям обработки информации: чтению, записи, исполнению
* по областям оперативной и долговременной памяти
* по времени и т.д.

Доступа должностных лиц к файлам осуществляется в соответствии с их функциональными обязанностями и полномочиями.

1. *Средства защиты операционной системы и программ пользователей.*

Защита операционной системы – наиболее приоритетная задача. Осуществляется запретом доступа в области памяти, в которых размещается операционная система.

Для защиты пользовательских программ применяется ограничение доступа к занимаемым этими программами памяти.

1. *Вспомогательные средства.*

К вспомогательным средствам программной защиты информации относятся:

* Программные средства контроля правильности работы пользователей,
* Программные уничтожители остатков информации
* Программы контроля работы механизма защиты
* Программы регистрации обращений к системе и выполнения действий с ресурсами
* Программы формирования и печати грифа секретности
* Программные средства защиты от компьютерных вирусов и др[2].

### 2.2.3.Криптографические средства защиты информации

*Криптографические средства защиты* – это методы специального шифрования данных, в результате которого их содержание становится недоступным без применения некоторой специальной информации и обратного преобразования.

Суть криптографической защиты заключается в преобразовании составных частей информации (слов, букв, слогов, цифр) с помощью специальных алгоритмов, либо аппаратных решений и кодов ключей, т.е. приведении ее к неявному виду. Для ознакомления с закрытой информацией применяется обратный процесс: декодирование (дешифрование). Использование криптографии является одним из распространенных методов , значительно повышающих безопасность передачи данных в сетях ЭВМ, данных, хранящихся в удаленных устройствах памяти, и при обмене информацией между удаленными объектами[2].

Более подробно вопросы криптографической защиты будут рассмотрены в разделе 5.

### 2.2.4.Организационные средства защиты информации

*Организационные средства защиты* – специальные организационно-технические и организационно-правовые мероприятия, акты и правила, осуществляемые в процессе создания и эксплуатации системы для организации и обеспечения защиты информации.

Организационные мероприятия осуществляют двойную функцию:

* Полное или частичное перекрытие каналов утечки информации,
* Объединение всех используемых средств защиты в целостный механизм.

Оргмеры по защите информации должны охватывать этапы проектирования, изготовления, испытаний, подготовки к эксплуатации и эксплуатации системы[2].

### 2.2.5.Законодательные средства защиты информации

*Законодательные средства защиты* – это законодательные акты, которые регламентируют правила использования и обработки информации, и устанавливают ответственность и санкции за нарушение этих правил.

Законодательные меры по защите информации от НСД заключаются в исполнении существующих в стране или введении новых законов, постановлений, положений и инструкций, регулирующих юридическую ответственность должностных лиц – пользователей и обслуживающего персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытку преднамеренного несанкционированного доступа к аппаратуре и информации. Таким образом цель законодательных мер – предупреждение и сдерживание потенциальных нарушителей[2].

## 2.3.Структура системы защиты информации

На основе принятой концепции средства защиты информации делятся на средства защиты от преднамеренного НСД (СЗИ ПНСД) и от случайного НСД (СЗИ СНСД). Средства управления защитой информации (СУЗИ) от НСД являются объединяющими, дающими возможность с помощью целенаправленных и взаимосвязанных функций в сочетании с наиболее полным охватом возможных каналов НСД объекта отдельными средствами защиты создать законченную и строгую систему защиты в комплексе средств автоматизации. Пример структуры такой системы приведен на рис.2.1.

СЗИ ПНСД включает 1-й контур защиты – систему контроля доступа на территорию объекта (СКДТО), 2-й контур защиты - систему контроля и разграничения доступа в помещение (СКРПД) и основной контур защиты (ОКЗ). СКДТО, содержащая систему охранной сигнализации (СОС) и контрольно-пропускные пункты (КПП), служит для ограничения доступа лиц на территорию объекта, а также совместно со специальными аппаратными решениями составляет средство защиты от побочных электромагнитных излучений и наводок.

Основной контур защиты перекрывает каналы доступа по периметру комплекса средств автоматизации (КСА). Система контроля вскрытия аппаратуры (СКВА) перекрывает доступ к внутреннему монтажу, технологическим пультам управления и кабельным соединениям. Система опознания и разграничения доступа к информации (СОРДИ) закрывает несанкционированный доступ и обеспечивает возможность контроля санкционированного доступа к информации законных пользователей и разграничения и разграничения их полномочий с учетом их функциональных обязанностей.

Средства защиты информации

Средства защиты от случайного НСД

Средства защиты от преднамеренного НСД

Средства управления защитой информации

Информационное обеспечение

Лингвистическое обеспечение

СКРДП

СЗИ АС

СПДИ

ФЗ ПО

ОКЗ

СКДТО

ФЗУЗИ

Оргмеры

СЗИ ПЭМИН

АРМ СБ

ЖУРД

СФК

УЗО КС

СОРДИ

СЗИН

САР

СКЦ ПО

ФЗ ПО

АЗКП

ТСБИ

СОС

КПП

АРДИ

СЩД

САП

СУСИ

СРП

САИН

СОБ

НКП

СТР

СКФ ЗИ

СИП

СФК КСА

СВПО

СЗКП

СЗОО

СКВА

Оргмеры

СЗПП

СИФЗ

УКВА

СВАРК

ЦСС

СЗР

Датчики

Оргмеры

Рис.2.1.Структурная схема защиты информации Средства вывода аппаратура из рабочего контура (СВАРК) обеспечивают блокировку НСД к информации при ремонте и профилактике аппаратуры. В числе средств основного контура применяются также средства защиты ресурсов (СЗР) и организационные меры. СЗР нацелены на недопущение блокировки пользователем-нарушителем работы других пользователей, а также для контроля и ограничения доступа пользователей к ресурсам.

Средства защиты информации на носителях (СЗИН) включают средства шифрования данных (СШД), средства уничтожения остатков информации на носителях (СУОИ), средства аутентификации информации на носителях (САИН), средства верификации программного обеспечения (СВПО) и организационно-технические мероприятия. Система контроля вскрытия аппаратуры включает датчики вскрытия, установленные на контролируемой аппаратуре, цепи сбора сигналов (ЦСС) и устройство контроля вскрытия аппаратуры (УКВА).

СОРДИ содержит терминал службы безопасности информации (ТСБИ), функциональные задачи программного обеспечения (ФЗ ПО), реализующие на программном уровне идентификацию и аутентификацию пользователей, а также разграничение их полномочий по доступу к информации. В целях защиты кодов паролей от НСД для них также должны быть предусмотрены средства защиты (СЗКП).

Средства защиты от случайного НСД включают средства повышения достоверности информации (СПДИ) и средства защиты информации от аварийных ситуаций (СЗИ АС). СПДИ содержат систему функционального контроля (СФК), устройство защиты от ошибок в каналах связи (УЗО КС), средства контроля целостности программного обеспечения (СКЦ ПО) и специальные технические решения (СТР). Они включают средства защиты от переадресации памяти (СЗПП), изоляции функциональных задач (СИФЗ) и другие технические решения.

Средства управления защитой информации содержат автоматизированное рабочее место службы безопасности (АРМ СБ) информации, ФЗ ПО, специально разработанные для выполнения управления защитой на программном уровне, включая ведение журнала учета и регистрации доступа (ЖУРД) и организационные мероприятия. АРМ СБ включает терминал безопасности, УКВА, аппаратуру записи кодов в физические ключи-пароли (АЗКП), необходимое количество ключей-паролей и аппаратуру регистрации и документирования информации (АРДИ). В дополнение к указанным средствам, выполненным на аппаратном и программном уровнях, в необходимых случаях применяются организационные меры[2].

## 2.4.Требования к защите информации в ЛВС подразделения

Чтобы обеспечить требуемый уровень безопасности информации в ЛВС подразделения, система безопасности должна иметь следующие средства:

* Средства идентификации и проверки полномочий
* Средства обеспечения защиты файлов
* Средства защиты ОС и программ пользователей
* Средства шифрования/дешифрования трафика сети
* Средства уничтожения остатков информации в системе
* Средства регистрации обращений к системе.

## 3.АНАЛИЗ ВОЗМОЖНОСТЕЙ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА ОС WINDOWS NT. ОБОСНОВАНИЕ ПРИМЕНЕНИЯ СПЕЦИАЛЬНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.

## 3.1.Обзор услуг Windows NT по обеспечению безопасности информации

Windows NT имеет средства обеспечения безопасности, встроенные в операционную систему. Рассмотрим наиболее значимые из них.

### 3.1.1.Централизованное управление безопасностью

Для повышения удобства Windows NT имеет централизованные средства управления безопасностью сети.

Имеется возможность установки области и связей доверия для централизации сетевого учета пользователей и другой информации, относящийся к безопасности, в одном месте, облегчая управление сетью и использование ее. При централизованном управлении безопасностью для каждого пользователя имеется только одна учетная карточка и она дает пользователю доступ ко всем разрешенным ему ресурсам сети. Можно использовать только один сетевой компьютер, чтобы проследить за активностью на любом сервере сети[1].

### 3.1.2.Управление рабочими станциями пользователей

*Профили пользователя* в Windows NT позволяют обеспечить большое удобство пользователям и в то же самое время ограничить их возможности, если это необходимо. Чтобы использовать профили пользователя для большей продуктивности, имеется возможность сохранить на сервере профили, содержащие все характеристики пользователя и установочные параметры, как например, сетевые соединения, программные группы и даже цвета экрана. Этот профиль используется всякий раз, когда пользователь начинает сеанс на любом компьютере с Windows NT так, что предпочитаемая им среда следует за ним с одной рабочей станции на другую. Для того, чтобы применять профили при ограничении возможностей пользователя, необходимо добавить ограничения к профилю, как например, предохранить пользователя от изменения программных групп и их элементов, делая недоступными части интерфейса Windows NT, когда пользователь будет регистрироваться в сети[1].

### 3.1.3.Слежение за деятельностью сети

Windows NT Server дает много инструментальных средств для слежения за сетевой деятельностью и использованием сети. ОС позволяет просмотреть серверы и увидеть, какие ресурсы они совместно используют; увидеть пользователей, подключенных к настоящему времени к любому сетевому серверу и увидеть, какие файлы у них открыты; проверить данные в журнале безопасности; записи в журнале событий; и указать, о каких ошибках администратор должен быть предупрежден, если они произойдут[1].

### 3.1.4.Начало сеанса на компьютере Windows NT

Всякий раз, когда пользователь начинает сеанс на рабочей станции Windows NT, экран начала сеанса запрашивают имя пользователя, пароль и домен. Затем рабочая станция посылает имя пользователя и пароль в определенный домен для идентификации. Сервер в этом домене проверяет имя пользователя и пароль в базе данных учетных карточек пользователей домена. Если имя пользователя и пароль идентичны данным в учетной карточке, сервер уведомляет рабочую станцию о начале сеанса. Сервер также загружает другую информацию при начале сеанса пользователя, как например установки пользователя, свой каталог и переменные среды.

По умолчанию не все учетные карточки в домене позволяют входить в систему серверов домена. Только карточкам групп администраторов, операторов сервера, операторов управления печатью, операторов управления учетными карточками и операторов управления резервным копированием разрешено это делать[1].

### 3.1.5.Учетные карточки пользователей

Каждый человек, который использует сеть, должен иметь *учетную карточку пользователя* в некотором домене сети. Учетная карточка пользователя содержит информацию о пользователе, включающую имя, пароль и ограничения по использованию сети, налагаемые на него. Имеется возможность также сгруппировать пользователей, которые имеют аналогичные работы или ресурсы, в группы; группы облегчают предоставление прав и разрешений на ресурсы, достаточно сделать только одно действие, дающее права или разрешения всей группе[1].

Табл.3.1 показывает содержимое учетной карточки пользователя.

Таблица 3.1

Учетная карточка пользователя

|  |  |
| --- | --- |
| **Элементы учетной карточки** | **Комментарий** |
| Username -Имя пользователя | Уникальное имя пользователя, выбирается при регистрации. |
| Password – пароль | Пароль пользователя. |
| Full name – полное имя | Полное имя пользователя |
| Logon hoursЧасы начала сеанса | Часы, в течение которых пользователю позволяется входить в систему. Они влияют на вход в систему сети и доступ к серверам. Так или иначе, пользователь вынужден будет выйти из системы, когда его часы начала сеанса, определенные политикой безопасности домена, истекут. |
| Logon workstationsРабочие станции начала сеанса | Имена рабочих станций, на которых пользователю позволяется работать. По умолчанию пользователь может использовать любую рабочую станцию, но возможно введение ограничений. |

Таблица 3.1(продолжение)

|  |  |
| --- | --- |
| **Элементы учетной карточки** | **Комментарий** |
| Expiration date -Дата истечения срока | Дата в будущем, когда учетную карточку автоматически исключают из базы, полезна при принятии на работу временных служащих. |
| Home directory -Собственный каталог | Каталог на сервере, который принадлежит пользователю; пользователь управляет доступом к этому каталогу. |
| Logon script Сценарий начала сеанса | Пакетный или исполняемый файл, который запускается автоматически, когда пользователя начинает сеанс. |
| Profile -Установки (параметры) | Файл, содержащий запись о параметрах среды рабочего стола (Desktop) пользователя, о таких, например, как сетевые соединения, цвета экрана и установочные параметры, определяющие, какие аспекты среды, пользователь может изменить.  |
| Account type Тип учетной карточки | Тип учетной карточки - глобальный или локальный. |

Кроме того, есть различные условия, которые или верны или неверны для каждой учетной карточки пользователя, как показано в табл.3.2.

Таблица 3.2

Дополнительные поля учетной карточки пользователя

|  |  |  |
| --- | --- | --- |
| **Условия учетной карточки** | **ПО УМОЛЧАНИЮ** | **Комментарии** |
| Изменение пароля в начале следующего сеанса? | ДА | Если ДА, пользователь изменяет пароль при следующем входе в систему. Затем эта величина устанавливается на НЕТ. |
| Пользователь не может изменить Пароль | НЕТ | Если ДА, пользователь не может изменить пароль. Это полезно для коллективных учетных карточек. |
| Пароль не имеет срока | НЕТ | Если ДА, учетная карточка пользователя игнорирует политику истечения срока пароля, установленную для домена и срок пароля никогда не истекает.  |
| Account Disabled – учетная карточка исключена | НЕТ | Если ДА, эта учетная карточка исключается и ее пользователь не может работать в сети. Она не удаляется из базы данных и может быть восстановлена. Это удобно для шаблонов учетных карточек. |

### 3.1.6.Журнал событий безопасности

Windows NT позволяет определить, что войдет в ревизию и будет записано в журнал событий безопасности всякий раз, когда выполняются определенные действия или осуществляется доступ к файлам. Элемент ревизии показывает выполненное действие, пользователя, который выполнил его, а также дату и время действия. Это позволяет контролировать как успешные, так и неудачные попытки каких-либо действий[1].

Табл.3.3 включает категории событий, которые могут быть выбраны для ревизии, а также события покрываемые каждой категорией.

Таблица 3.3

Категории событий для ревизии

|  |  |
| --- | --- |
| Категория | События |
| Начало и конец сеанса | Попытки начала сеанса, попытки конца сеанса; создание и завершение сетевых соединений к серверу |
| Доступ к файлам и объектам | Доступы к каталогу или файлу, которые устанавливаются для ревизии в диспетчере файлов; использование принтера, управление компьютером |
| Использование прав пользователя | Успешное использование прав пользователя и неудачные попытки использовать права, не назначенные пользователям |
| Управление пользователями и группами | Создание, удаление и модификация учетных карточек пользователя и групп |
| Изменения полиса безопасности | Предоставление или отменена прав пользователя пользователям и группам, установка и разрыв связи доверия с другими доменами |
| Перезапуск, выключение и система | Остановка и перезапуск компьютера, заполнение контрольного журнала и отвержение данных проверки если контрольный журнал уже полон |
| Трассировка процесса | Начало и остановка процессов в компьютере |

Табл.3.4 показывает типы доступа к каталогам и файлам, которые можно проверить.

Таблица 3.4

Типы доступа к каталогам и файлам

|  |  |
| --- | --- |
| **Доступ к каталогу** | **Доступ к файлу** |
| Отображение имен файлов в каталоге | Отображение данных, хранимых в файле |
| Отображение атрибутов каталога | Отображение атрибутов файла |
| Изменение атрибутов каталога | Отображение владельца файла и разрешений |
| Создание подкаталогов и файлов | Изменение файла |
| Переход в подкаталогах каталога | Изменение атрибутов файла |
| Отображение владельца каталога и разрешений | Запуск файла |
| Удаление каталога | Удаление файла |
| Изменение разрешений каталога | Изменение файловых разрешений |
| Изменение владельца каталога | Изменение владельца файла |

### 3.1.7.Права пользователя

Права пользователя определяют разрешенные типы действий для этого пользователя. Действия, регулируемые правами, включают вход в систему на локальный компьютер, выключение, установку времени, копирование и восстановление файлов сервера и выполнение других задач.

В доменах Windows NT Server права предоставляются и ограничиваются на уровне домена; если группа находится непосредственно в домене, участники имеют права во всех первичных и резервных контроллерах домена. В каждой рабочей станции Windows NT и в каждом компьютере Windows NT Server, который не является контроллером домена, предоставленные права применяются только к этому единственному компьютеру[1].

### 3.1.8.Установка пароля и политика учетных карточек

Для каждого домена можно определить все аспекты политики пароля: минимальную длину пароля (по умолчанию 6 символов), минимальный и максимальный возраст пароля (по умолчанию устанавливается 14 и 30 дней) и исключительность пароля, который предохраняет пользователя от изменения его пароля на тот пароль, который пользователь использовал недавно (по умолчанию должен предохранить пользователей от повторного использования их последних трех паролей).

Дается возможность также определить и другие аспекты политики учетных карточек:

1. Должна ли происходить блокировка учетной карточки.
2. Должны ли пользователи насильно отключаться от серверов домена по истечении часов начала сеанса.
3. Должны ли пользователи иметь возможность входа в систему, чтобы изменить свой пароль.

Когда разрешена блокировка учетной карточки, тогда учетная карточка блокируется в случае нескольких безуспешных попыток начала сеанса пользователя, и не более, чем через определенный период времени между любыми двумя безуспешными попытками начала сеанса. Учетные карточки, которые заблокированы, не могут быть использованы для входа в систему.

Если пользователи принудительно отключаются от серверов, когда время его сеанса истекло, то они получают предупреждение как раз перед концом установленного периода сеанса. Если пользователи не отключаются от сети, то сервер произведет отключение принудительно. Однако отключения пользователя от рабочей станции не произойдет.

Если от пользователя требуется изменить пароль, то, когда он этого не сделал при просроченном пароле, он не сможет изменить свой пароль. При просрочке пароля пользователь должен обратиться к администратору системы за помощью в изменении пароля, чтобы иметь возможность снова входить в сеть. Если пользователь не входил в систему, а время изменения пароля подошло, то он будет предупрежден о необходимости изменения, как только он будет входить и помощь администратора ему будет не нужна[1].

## 3.2.Обоснование недостаточности встроенных средств защиты информации ОС Windows NT

При всех неоспоримых положительных качествах, встроенных средств обеспечения безопасности Windows NT в нашем случае их не достаточно.

Этот вывод сделан на основании того, что не все требования, перечисленные в разделе 2.4, выполняются встроенными средствами безопасности ОС Windows NT, а именно:

* нет возможности шифрования трафика сети;
* дополнительной идентификации пользователей;
* затирания остатков информации в системе.

# 4.ВЫБОР ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Так как Windows NT не может обеспечить требуемый уровень безопасности данных в локальной вычислительной сети нашего подразделения, то логичным является путь установки дополнительных средств защиты. Сегодня на рынке присутствует достаточное количество дополнительных средств защиты данных, требующихся нашей системе. Проанализируем возможности, предоставляемые этими средствами, и сделаем оптимальный выбор.

## 4.1.Обзор комплексов защиты информации

### 4.1.1.Комплекс “Аккорд”

В состав комплекса входит одноплатный контроллер, вставляемый в свободный слот компьютера, контактное устройство (съемник информации), программное обеспечение и персональные идентификаторы DS199x Touch Memory в виде таблетки. Съемник устанавливается на передней панели компьютера, а идентификация осуществляется прикосновением идентификатора (таблетки) к съемнику. Аутентификация выполняется до загрузки операционной системы. Дополнительно может быть поставлена библиотека программ для подключения средств шифрования и электронной подписи[2].

Таким образом, комплекс “Аккорд” не предоставляет всех необходимых нам услуг по защите информации. Шифрование и затирание остатков информации на носителях может быть произведено при помощи дополнительных утилит, аналогичных Diskreet и Wipeinfo из пакета Norton Utilities.

### 4.1.2.Комплекс Dallas Lock

В соответствии со спецификацией версия Dallas Lock 3.1 должна обеспечивать полномасштабную защиту рабочей станции, а также связь со станцией мониторинга.

Комплекс предусматривает регистрацию пользователя на рабочей станции и вход его в сеть посредством касания электронной карточки Touch Memory. Число вариантов серийных номеров – 48 триллионов.

Dallas Lock обеспечивает:

* возможность доступа к компьютеру и загрузки операционной системы только по предъявлении личной электронной карты пользователя и вводе личного пароля,
* многоуровневое разграничение доступа по отношению к ресурсам компьютера,
* защиту операционной системы,
* ведение системных журналов событий,
* установку для пользования опции гарантированного стирания файлов при их удалении,
* защиту собственных файлов и контроль целостности среды[2].

### 4.1.3.Комплекс Secret Net NT

Ассоциация “Информзащита” предлагает систему защиты Secret Net, предназначенную для защиты хранимой и обрабатываемой информации на персональных компьютерах в ЛВС от НСД и противодействия попыткам нарушения нормального функционирования ЛВС и прикладных систем на ее основе. В качестве защищаемого объекта выступает ЛВС персональных ЭВМ типа IBM PC/AT и старше, объединенных при помощи сетевого оборудования Ethernet, Arcnet или Token-Ring. Система включает средства:

* идентификации и аутентификации пользователей (в том числе и при использовании карт Touch Memory и Smart Card),
* разграничения доступа к ресурсам,
* контроля целостности,
* регистрации событий в журнале безопасности,
* затирания остатков данных на носителях информации,
* шифрования трафика сети,
* управления средствами защиты и др.

Система Secret Net имеет сертификат Гостехкомиссии РФ[3].

### 4.1.4.Выбор комплекса защиты информации

Проанализировав возможности рассмотренных выше комплексов защиты информации в локальных сетях, можно прийти к выводу, что лишь Secret Net NT удовлетворяет всем трем пунктам наших требований, изложенных в разделе 3.2.

## 4.2.Обзор возможностей программно-аппаратного комплекса Secret Net NT

Не умаляя достоинств Secret Net NT, надо сразу сказать, что эта система не сможет решить ВСЕХ проблем по созданию комплексной защиты компьютерных систем. Этого не может сделать никакое отдельно взятое техническое средство защиты, так же как и любая совокупность таких средств. Объясняется это тем, что создание комплексной системы защиты организации, кроме применения технических (аппаратно-программных) средств, предполагает принятие специальных мер правового и административного характера и обеспечение непрерывной организационной поддержки функционирования установленных средств защиты специальным персоналом.

Надо совершенно четко понимать, что система Secret Net NT - это всего лишь инструмент, позволяющий сотрудникам службы компьютерной безопасности значительно проще и надежнее решать одну из стоящих перед ними задач - задачу разграничения доступа должностных лиц к ресурсам компьютера (аппаратным, программным, информационным) в строгом соответствии с принятой в организации политикой безопасности.

Для эффективного применения системы Secret Net NT необходимо правильно ее установить и настроить, то есть назначить пользователям компьютера полномочия по доступу к ресурсам в соответствии с разработанными ранее (и возможно уточненными в ходе самой настройки системы защиты) документами. Требуемые полномочия назначаются пользователям путем соответствующей настройки средств парольной защиты, атрибутного и полномочного механизмов управления доступом к ресурсам компьютера.

Чаще всего устанавливать систему Secret Net NT приходится на компьютер, на котором уже реально работают пользователи. Для того, чтобы работы по ее установке и настройке не привели к временному нарушению их нормальной работы, в Secret Net NT предусмотрен целый ряд специальных возможностей и режимов. К ним относятся:

1. поддержка технологии поэтапной установки компонент системы защиты Secret Net NT;
2. возможность управления подключением различных защитных механизмов;
3. наличие специального "мягкого" режима функционирования механизмов защиты.

Перечисленные выше возможности позволяют плавно повышать степень защищенности автоматизированной системы, не нарушая ее нормального функционирования[3].

Далее остановимся более подробно на некоторых наиболее полезных нам возможностях комплекса Secret Net NT.

### 4.2.1.Дополнительная идентификация

Имеется возможность дополнительной идентификации пользователя при входе в систему с предъявлением персонального идентификатора.

В процессе загрузки системы на экране компьютера появляется запрос на предъявление устройства идентификации (Touch Memory или Smart Card). Система Secret Net NT считывает имя, пароль и ключ с идентификатора и продолжает загрузку операционной системы[3].

### 4.2.2.Ключевой диск пользователя

При операциях с зашифрованными файлами и каталогами все приложения системы Secret Net NT (сервер управления доступом, утилиты) используют секретные ключи, записанные на сменных носителях (дискетах, магнитооптических дисках) – ключевых дисках[3].

### 4.2.3.Управление регистрацией событий

В системном журнале фиксируются различные события, происходящие на рабочей станции. От уровня регистрации (количества регистрируемых событий) зависит время, потраченное на запись сообщений в системный журнал и, соответственно, размер системного журнала (место занимаемое на диске). Поэтому, разумно ограничить список регистрируемых событий, например регистрировать только сбойные события.

В системе защиты Secret Net NT администратор может регистрировать успешные или сбойные события следующих типов:

1. вход/выход в систему;
2. доступ к файлам и объектам;
3. применение прав пользователей;
4. управление пользователями и группами пользователей;
5. изменение политики безопасности;
6. рестарт, перезагрузка, выключение компьютера и системные события;
7. события, связанные со слежением за процессом[3].

### 4.2.4.Автоматическое затирание удаляемых данных

Администратор может установить для пользователя возможность автоматического затирания на диске содержимого удаляемых файлов псевдослучайной числовой последовательностью. Многократное повторение затирания данных на диске позволяет предотвратить восстановление удаленных файлов. Количество повторений операции затирания может быть выбрано по своему усмотрению[3].

## 4.3.Алгоритм функционирования специальных средств защиты информации

На рис.4.1 показан алгоритм функционирования специальных программно-аппаратных средств защиты информации в ЛВС (Secret Net NT).

Рис.4.1. Схема алгоритма функционирования специальных программно-аппаратных средств защиты информации

На рис.4.1 показана типичная процедура входа пользователя в систему с применением двойной идентификации (пароль + дополнительное средство, например Smart Card). Число попыток идентификации ограничено: при превышении их количества рабочая станция будет заблокирована.

Все действия пользователя регистрируются в системном журнале, содержимое которого может быть в последствии просмотрено и проанализировано.

При возникновении события несанкционированного доступа к информации, происходит оповещение администратора безопасности системы, а он уже принимает решение о принятии соответствующих мер.

# 5.Шифрование трафика сети и настройка сервера безопасности

## 5.1.Обзор и классификация методов шифрования информации

Для преобразования (шифрования) информации обычно используется некоторый алгоритм или устройство, реализующее заданный алгоритм, которые могут быть известны широкому кругу лиц. Управление процессом шифрования осуществляется с помощью периодически меняющегося кода ключа, обеспечивающего каждый раз оригинальное представление информации при использовании одного и того же алгоритма или устройства. Знание ключа позволяет просто и надежно расшифровать текст. Однако, без знания ключа эта процедура может быть практически невыполнима даже при известном алгоритме шифрования.

Даже простое преобразование информации является весьма эффективным средством, дающим возможность скрыть ее смысл от большинства неквалифицированных нарушителей. Структурная схема шифрования информации представлена на рис.5.1.

Ключ

Ключ

Открытый текст

Открытый текст

Устройство дешифрования

Устройство шифрования

*Передатчик*

*Приемник*

Рис.5.1.Шифрование информации

Для построения средств защиты от НСД необходимо иметь представление о методах криптографии. Их классификация приведена на рис.5.2.

Криптографическое закрытие информации

Другие виды

Кодирование

Шифрование

Символьное

Смысловое

Сжатие- расширение

Рассечение-разнесение

По таблицам

Смысловое

По кодовому алфавиту

Механическое

Замена (подстановка)

Перестановка

Аналитическое преобразование

Комбинированные

Гаммирование

Простая (одноалфавитная)

Замена + перестановка

Многоалфавитная одноконтурная монофоническ.

Замена +гаммирование

Перестановка+гаммир.

Многоалфавитная одноконтурная обыкновенная

Гаммирование+гаммир.

Многоалфавитная многоконтурная

С бесконечной гаммой

С конеч. длинной гаммой

Простая

С конеч. короткой гаммой

По правилам алгебры матриц

Усложненная по маршруту

Усложненная по таблице

По особым зависимостям

Рис.5.2.Классификация методов криптографии

Сам процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно, однако аппаратная реализация обладает рядом преимуществ, главным из которых является высокая производительность.

Сформулирована следующая система требований к алгоритму шифрования:

* зашифрованный текст должен поддаваться чтению только при наличии ключа шифрования,
* число операций для определения использованного ключа шифрования по фрагменту шифрованного текста и соответствующему ему открытого текста, должно быть не меньше общего числа возможных ключей,
* знание алгоритма шифрования не должно влиять на надежность защиты,
* незначительные изменения ключа шифрования должны приводить к существенному изменению вида зашифрованного текста,
* незначительные изменения шифруемого текста должны приводить к существенному изменению вида зашифрованного текста даже при использовании одного и того же ключа,
* длина шифрованного текста должна быть равна длине исходного текста,
* любой ключ из множества возможных должен обеспечивать надежную защиту информации,
* алгоритм должен допускать как программную, так и аппаратную реализацию[2].

## 5.2.Системы шифрования с секретным и открытым ключом

Современные широко применяемые методы шифрования можно разделить на два наиболее общих типа: с секретным ключом и с открытым ключом.

Шифрование с секретным ключом симметрично – ключ, с помощью которого текст шифруется, применяется и для его дешифровки.

Шифрование с открытыми ключами осуществляется с помощью двух ключей, поэтому оно относится к асимметричным системам шифрования. Открытый ключ не является секретным; более того, его доступность для всех и каждого, например за счет публикации в каталоге или включения в незащищенное сообщение электронной почты, имеет принципиальное значение для функционирования всей системы. Другой ключ, личный, служит для шифрования текстов, дешифруемых с помощью открытого ключа[4].

Криптографические системы с открытым ключом используют необратимые или односторонние функции, для которых при заданном значении Х относительно просто вычислить значение f(x), однако если y=f(x), то нет простого пути для вычисления значения Х. Другими словами, чрезвычайно трудно рассчитать значение обратной функции[2].

На практике криптографические системы с секретными ключами, как правило, быстрее систем с открытыми ключами, обеспечивающими ту же степень защиты.

## 5.3.Алгоритм шифрования трафика сети

В системе шифрования трафика сети комплекса Secret Net используется метод шифрования с секретным ключом. В ее основу положен алгоритм, основанный на известном стандарте DES, и соответствующий ГОСТ 28147-89.

Суть алгоритма заключается в линейном преобразовании: S = L \* t, где L – невырожденная матрица случайного линейного преобразования бит. И хотя расшифровывание в этом случае придется осуществлять решением систем линейных уравнений, но каждый бит шифровки начинает уже зависеть от каждого бита текста. Шифры на основе этого преобразования называют *скремблерами* (взбивателями). Для того, чтобы матрица L была невырожденной, случайной и при расшифровывании не нужно было производить много вычислений, американскими криптографами был предложен оригинальный алгоритм. Входной блок данных делится на левую L’ и правую R’ части. После этого формируется выходной массив так, что его левая часть L” представлена правой частью R’ входного, а правая часть R” формируется как сумма L’ и R’ операцией XOR. Далее, выходной массив шифруется перестановкой с заменой. После нескольких таких взбиваний каждый бит выходного блока может зависеть от каждого бита сообщения (рис.5.3.)[5].

Входные данные

Начальная перестановка

Ln=Rn-1

K2

R1=L0 ⊕ f(R0,K1)

L1=R0

K1

L0

R0

**………………**

Kn

Rn=Ln-1 ⊕ f(Rn-1,Kn)

Результат

Обратная начальная перестановка

Рис.5.3.Схема алгоритма шифрования трафика сети.

## 5.4.Сервер безопасности

### 5.4.1.Принципы работы сервера безопасности

В целях обеспечения защиты данных Secret Net следует следующим принципам:

1. Пользователь должен идентифицировать себя только раз в начале сессии. Это включает ввод имени и пароля клиента.
2. Пароль никогда не посылается по сети в открытом виде. Он всегда зашифрован. Дополнительно пароль никогда не хранится на рабочей станции или сервере в открытом виде.
3. Каждый пользователь имеет пароль, и каждая служба имеет пароль.
4. Единственным устройством, которое знает все пароли, является *сервер безопасности*. Этот сервер работает под серьезной охраной.

Рассмотрим схему работы сервера безопасности (рис.5.4.):

1. Пользователь вводит имя.
2. Перед вводом пароля выдается через сеть сообщение на сервер аутентификации. Это сообщение содержит имя пользователя вместе с именем Ticket-Granting Server (TGS). Это сообщение не нуждается в шифровании, так как знание имен в сети необходимо всем для электронной почты.

Сервер

WS

(7)

(6)

(8)

(3)

(4)

(2)

(1)

(10)

(11)

(5)(9)

TGS

Сервер аутентификации

Рис.5.4. Система распределения ключей Secret Net

1. Сервер аутентификации по имени пользователя и имени TGS сервера извлекает из базы данных ключи для каждого из них.
2. Сервер аутентификации формирует ответ, который содержит Ticket (билет), который гарантирует доступ к запрашиваемому серверу. Ticket всегда посылается в закрытом виде. Ticket содержит временную марку и дату создания. Сервер аутентификации шифрует этот ticket , используя ключ TGS сервера (полученного на шаге 3). Это дает sealed ticket (запечатанный билет), который передается на рабочую станцию в зашифрованном виде (на ключе пользователя).
3. Рабочая станция, получив зашифрованное сообщение, выдает запрос на ввод пароля. Пароль пользователя используется внутренним дешифратором для расшифровывания сообщения. Затем ключ пользователя удаляется из памяти. На этот момент на рабочей станции имеется sealed ticket.

 *Рассмотрим сценарий, когда пользователь хочет воспользоваться некоторой службой сети, например, запросить некий сервер (end server). Каждый запрос этой формы требует, прежде всего, получения ticket для данного сервера.*

1. Рабочая станция создает сообщение, состоящее из sealed-ticket, sealed-authenticator и имени сервера, которое посылается TGS. Authenticator состоит из login-name, WS-net-address и текущего времени. Закрытый аутентификатор (sealed-authenticator) получается шифрованием.
2. TGS, получив сообщение, прежде всего, расшифровывает sealed-ticket и sealed-authenticator, используя ключ TGS. Таким образом, TGS получает все параметры для проверки достоверности:
* Login-name,
* TGS-name,
* Сетевой адрес рабочей станции.

Наконец, сравнивается текущее время в authenticator, чтобы определить, что сообщение сформировано недавно. Это требует, чтобы все рабочие станции и сервера держали время в пределах допустимого интервала. TGS по имени сервера из сообщения определяет ключ шифрования сервера.

1. TGS формирует новый ticket, который базируется на имени сервера. Этот ticket шифруется на ключе сервера и посылается на рабочую станцию.
2. Рабочая станция получает сообщение, содержащее sealed-ticket, который она расшифровать не может.
3. Рабочая станция посылает сообщение, содержащее sealed-ticket, sealed-authenticator и имя сервера (сообщение не шифруется).
4. Сервер принимает это сообщение и прежде всего дешифрует sealed-ticket, используя ключ, который только этот сервер и Secret Net знают.

Сервер далее расшифровывает authenticator и делает проверку также как в пункте 7.

Ticket и аутентификаторы являются ключевыми моментами для понимания применения сервера безопасности. Для того, чтобы рабочая станция использовала сервер, требуется билет (ticket). Все билеты, кроме первого, получаются из TGS. Первый билет является специальным: это билет для TGS и он получается из сервера аутентификации.

Билеты, получаемые рабочей станцией, не являются исчерпывающей информацией для нее. Они зашифрованы на ключе сервера, для которого они будут использованы. Каждый билет имеет время жизни. Когда билет уничтожается, пользователь должен идентифицировать себя снова, введя свое имя и пароль. Чтобы выполнить это уничтожение, каждый билет содержит время его создания (выпуска) и количество времени, в течении которого он действителен.

В отличие от билета, который может повторно использоваться, новый аутентификатор требуется каждый раз, когда клиент инициирует новое соединение с сервером. Аутентификатор несет временной штамп (метку), и уничтожается в течение нескольких минут после создания. Вот почему мы предполагаем, что все рабочие станции и серверы должны поддерживать синхронизацию часов. Точность этой синхронизации и размер сети определяют максимум рационального времени жизни аутентификатора.

Сервер должен поддерживать историю предыдущих запросов клиента, для которых временная метка аутентификатора еще действительна (т.е. историю всех запросов внутри последних нескольких минут). Таким образом, сервер может отсечь дубликаты запросов, которые могут возникнуть в результате украденных билетов и аутентификаторов.

Поскольку, как билет, так и аутентификатор содержат сетевой адрес клиента, другая рабочая станция не может использовать украденные копии без изменения их сущности, связанной с сетевым адресом владельца. Далее, поскольку аутентификатор имеет короткое время жизни и действителен только один раз, то взломщик должен проделать это до смерти аутентификатора, обеспечив также уверенность, что оригинальная копия билета и аутентификатора не достигнет нужного конечного сервера, и модифицировать их сетевой адрес, чтобы выглядеть как истинный клиент.

Поскольку сервер подтверждает запрос клиента на обслуживание, то клиент и сервер разделяют одинаковый ключ шифрования. При желании клиент и сервер могут шифровать все данные их сессии, используя этот ключ, или они могут выбрать не шифровать данные вообще.

Поскольку сервер удостоверил клиента, остальные шаги служат для удостоверения сервера. Это решает проблему неперсонифицированного вторжения в качестве сервера (т.е. подмены сервера). Клиент в этом случае требует, чтобы сервер послал назад сообщение, состоящее из временного штампа и аутентификатора клиента вместе со значением временной марки. Это сообщение зашифровано. Если сервер поддельный, он не знает действительного ключа шифрования сервера.

Таким образом, вторгнуться в систему можно только тогда, когда взломщик может узнать имя и пароль клиента.

### 5.4.2.Настройка сервера безопасности

Администратор может изменить следующие параметры настройки сервера управления доступом (как это показано на рис.5.5):

1. максимальное количество администраторов системы защиты, одновременно работающих в сети (поле “Количество администраторов, одновременно находящихся в сети”);
2. период времени, в течение которого сервер управления доступом ожидает подтверждения активности клиентских компьютеров. Если в течение указанного периода такое подтверждение не получено, сервер управления доступом отключает данный компьютер от сети. Данный параметр может принимать значения от 10 до 60 секунд (поле “Период обновления информации о клиенте, с”)[6].

Рис.5.5.Настройка сервера безопасности.

# 6.ВЫБОР И РАСПРЕДЕЛЕНИЕ ПАРОЛЕЙ ЗАЩИТЫ. МОНИТОРИНГ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.

## 6.1.Выбор паролей

Пароль – это секретное слово, известное только конкретному пользователю. При правильном использовании пароль удостоверяет личность пользователя, входящего в компьютерную сеть[7].

Пользователь выбирает кодовую комбинацию из нескольких литер, записывает ее в память ЭВМ и затем, чтобы получить доступ к вычислительной системе, он должен будет ввести пароль с клавиатуры. Многие системы при этом выключают “печатающую головку”, так что вводимый пароль не отображается на экране дисплея[8].

Объектом аутентификации может быть некоторый объем знаний человека. При выборе пароля естественно возникает вопрос, каким должен быть его размер и стойкость к несанкционированному подбору?

Чем больше длина пароля, тем большую безопасность будет обеспечивать система, так как потребуются большие усилия для его подбора. Это обстоятельство можно представить в терминах ожидаемого времени раскрытия пароля или ожидаемого безопасного времени. Ожидаемое безопасное время (Тб)- полупроизведение числа возможных паролей и времени, требуемого для того, чтобы попробовать каждый пароль из последовательности запросов. Представим эти формулы:

 (6.1)

Где t – время, требуемое на попытку введения пароля, равное E/R;

R – скорость передачи (символы в минуту) в линии связи;

Е – число символов в передаваемом сообщении при попытке получить доступ (включая пароль и служебные символы);

S – длина пароля;

А – число символов в алфавите, из которых составляется пароль.

Если после каждой неудачной попытки подбора автоматически предусматривается некоторая задержка (например, 10 секунд), то безопасное время резко увеличивается. Если в дополнение к R,E,M и А примем, что пароль может быть раскрыт посторонним лицом с вероятностью Р , то получим формулу Андерсона:

 (6.2)

s

Если R,E,M и A фиксированы, то каждое значение S будет давать различную вероятность Р правильного его отгадывания. Если мы хотим построить систему, где незаконный пользователь имел бы вероятность отгадывания пароля не большую, чем Р , то следует выбрать такое S, которое бы удовлетворяло выражению (6.2).

Нетрудно заметить, что в выражениях (6.1) и (6.2) величина S является показателем степени и, следовательно, оказывает большое влияние на безопасное время и вероятность раскрытие пароля[2].

Проведем расчет длины пароля для различных категорий пользователей сети нашего подразделения. Допустим, что будет применяться стандартный английский алфавит, т.е. А=26; период времени подбора пароля М=3 месяца; скорость передачи R=600 символов в минуту; число символов в передаваемом сообщении Е=20.

Таблица 6.1

Выбор длины паролей

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Категория****пользователей** | **Вероятность угадывания****Р** | **Длина****пароля****S** |
| 1 | Администратор |  0.0001 | **8** |
| 2 | Продвинутый пользователь |  0.001 | **7** |
| 3 | Сотрудник |  0.05 | **6** |

Выбор длины пароля в значительной степени определяется развитием технических средств, их элементной базы и быстродействия. В настоящее время широко применяются пароли, где S>10. В связи с этим возникают вопросы: как и где хранить пароль и как связать его с аутентификации пользователя? Ведь хорошо известно, что, несмотря на самые строгие предупреждения о недопустимости хранения пароля на листке бумаги на рабочем месте, многие сотрудники именно так и поступают, причем, при увеличении его длины, их непрерывно возрастает. Это объясняется естественной боязнью человека забыть пароль в самый неподходящий момент.

На помощь приходит комбинированная система, в которой код пароля состоит из двух частей. Первая часть состоит из 3-4х знаков, которые легко могут быть запомнены человеком. Вторая часть содержит количество знаков, определяемое требованиями к защите и возможностями технической реализации системы, она помещается на физический носитель и определяет ключ-пароль, расчет длины которого ведется по указанной выше методике[2].

Худшими паролями являются очевидные слова, инициалы, географические названия и имена людей, телефонные номера, даты рождения или полные слова какого-либо языка: в языке ограниченное число слов и компьютер сможет их достаточно быстро перебрать[9]. В Приложении 1 приведен список стандартных паролей адаптированных к условиям России, применение которых крайне нежелательно.

Приведем несколько правил формирования “правильных” паролей:

* пароль должен быть неожиданным, лучше – случайным,
* при малейшей опасности желательно сменить все пароли,
* не желательно использование одного и того же пароля в разных системах[5].

В качестве пароля может быть использован набор ответов на M стандартных и N ориентированных на пользователя вопросов. Этот метод получил название “вопрос - ответ”. Когда пользователь делает попытку включиться в работу, система случайным образом выбирает и задает ему некоторые (или все) из этих вопросов. Пользователь должен дать правильные ответы на все вопросы, чтобы получить доступ к информации.

При увеличении длины пароля нельзя увеличивать периодичность его смены на новые значения более 1 года. Коды паролей необходимо менять обязательно, так как за большой период времени увеличивается вероятность их перехвата путем прямого хищения носителя, снятия его копии, принуждения человека. Выбор периодичности необходимо определять из конкретных условий работы системы, но не реже одного раза в год. Причем дата замены и периодичность должны носить случайный характер[2].

## 6.2.Мониторинг несанкционированного доступа

На этапе эксплуатации администрация безопасности выполняет следующие функции:

1. поддерживает средства защиты в работоспособном состоянии и периодически контролирует корректность их работы;
2. производит изменения в настройке средств защиты на основании и в полном соответствии с изменениями в плане защиты. Они могут быть вызваны различными причинами, например, изменениями списка пользователей, состава сотрудников и их должностных или функциональных обязанностей, расширением номенклатуры используемых технических и программных средств, задач и т.п. Рекомендуется проводить эти изменения в системе только по утвержденным документам;
3. осуществляет текущий контроль над работой пользователей системы;
4. анализирует содержимое журналов регистрации событий, формируемых средствами защиты, и т.п.

### 6.2.1.Текущий контроль над работой пользователей системы

Администратор может управлять эксплуатацией каждой рабочей станции с помощью диалога *"Монитор"* утилиты *NetAdmin*. Для каждого защищаемого компьютера (в соответствии с приобретенным комплектом системы Secret Net NT) предусмотрен специальный знак - экран, под которым указано имя компьютера в системе. Текущее состояние компьютера в системе отображается с помощью цвета экрана и специальных символов на нем, приведенных в табл.6.2.

Таблица 6.2

Символы, отображающие текущее состояние рабочей станции в системе Secret Net NT

|  |  |
| --- | --- |
| **Цвет**  | **Состояние рабочей станции** |
| Черный | Компьютер не активен |
| Зеленый | Компьютер активен |
| Желтый | Рабочая станция не подтвердила свое существование хотя бы один раз |
| **Символ** | **Состояние рабочей станции** |
|  | Пользователь вошел в систему |
|  | Установлен режим шифрования соединений |
|  | Установлен режим строгой аутентификации |
|  | Компьютер блокирован |
|  | Изменена конфигурация компьютера |
|  | Включен хранитель экрана |
|  | Произошло переполнение системного журнала |
|  | Произошло событие НСД |
|  | Произошло событие НСД при выключенном сервере управления доступом |

Администратор может получить информацию о текущем состоянии рабочей станции и о ее пользователе в данный момент времени и, при необходимости, может приостановить работу любого пользователя системы на определенном компьютере.

Для оперативного управления в системе защиты Secret Net NT предусмотрена возможность блокировки, выключения и перезагрузки любой рабочей станции системы[3].

### 6.2.2.Анализ журналов регистрации событий

В системном журнале содержится список всех событий, которые произошли на рабочей станции, в соответствии с установленным режимом регистрации. При перезагрузке (начальной загрузке) рабочей станции, подключении любого пользователя с этой станции к сети, либо по требованию администратора системный журнал перемещается на сервер управления доступом и хранится в базе данных на сервере. После этого его содержимое можно анализировать при помощи утилиты *NetAdmin*. Имеется возможность просмотреть системный журнал полностью или запросить выборку событий. Выборка может быть сделана по имени компьютера, имени пользователя и дате (интервалу дат).

В системном журнале содержатся следующие сведения:

1. дата и время события (колонка ***"****Время****"***);
2. пользователь, в течение работы которого произошло событие (колонка ***"****Пользователь****"***);
3. рабочая станция, на которой произошло событие (колонка *"Компьютер"*);
4. категория события (колонка *"Категория"*);
5. описание события (колонка *"Сообщение"*).

При отображении содержимого системного журнала записи каждого типа выделены своим цветом: обычные события регистрации имеют черный цвет, вход пользователя в систему - зеленый, события НСД - красный, события расширенной регистрации - фиолетовый, сетевые события - зеленый и т.д.[3].

Проводя анализ системного журнала безопасности, администратор может выявить пользователей, наиболее часто совершающих попытки несанкционированного доступа. На основе этих данных может быть сделан вывод о преднамеренном или случайном характере НСД в случае каждого пользователя.

В рамках данного дипломного проекта была создана программа, предоставляющая широкие возможности по просмотру и анализу журналов безопасности.

### 6.2.3.Структурная схема мониторинга нсд

На рис.6.1 показана схема функционирования системы мониторинга событий НСД. На ней отражено слежение за несанкционированным доступом к информации не только программным путем. Необходим также контроль несанкционированного вскрытия аппаратуры и проникновения в помещения. Вся эта информация должна попадать на АРМ администратора безопасности системы, который должен принимать адекватные меры при возникновении НСД.

Рис.6.1. Структурная схема системы мониторинга несанкционированного доступа

## 6.3.программа анализа журнала безопасности

### 6.3.1.Предпосылки к созданию программы

Системный журнал безопасности – огромный резервуар, хранящий многие килобайты записей о событиях в сети. Проводя тщательный анализ журнала, администратор безопасности может существенно повысить эффективность своей работы.

К сожалению, штатные средства Secret Net NT позволяют лишь просматривать содержимое журнала (при желании возможна выборка событий некоторой категории, событий за промежуток времени, а также связанных с конкретным пользователем или компьютером в сети). Анализ предоставленной информации целиком ложится на плечи администратора, хотя с этим гораздо эффективней могла бы справиться ЭВМ. Известно, что человек лучше воспринимает информацию, когда она представлена не в виде списков или таблиц, а в виде графиков и диаграмм, поэтому логичным было бы отображать результаты анализа журнала в виде именно в таком виде.

Вышесказанное подводит нас к необходимости создания приложения, реализующего эти функции.

### 6.3.2.выбор среды программирования

На текущий момент имеется несколько развитых языков программирования, позволяющих создавать полноценные программы, предназначенные для работы в среде Windows NT, но основными конкурирующими платформами стали Delphi и C++. В последнее время мы стали свидетелями прогресса в области программирования: появились программные продукты, реализующие концепцию быстрой графической разработки программ (rapid application development - RAD). Примерами таких сред программирования для C++ могут являться Optima++ фирмы Powersoft и C++Builder фирмы Borland[10].

C++ Builder для Windows 95 и Windows NT – выпущенное в 1997г. компанией Borland International новое средство быстрой разработки корпоративных информационных систем. Это средство сочетает в себе удобства визуальной среды разработки, объектно-ориентированный подход, разнообразные возможности повторного использования кода, открытую архитектуру и высокопроизводительный компилятор языка С++[11].

Интерфейс С++ Builder в значительной мере повторяет модель Delphi с инструментальной панелью компонентов (рис.6.2).

Рис.6.2.Интерфейс Borland C++ Builder.

Программирование в основном сводится к проектированию форм из элементов графической библиотеки компонентов (Visual Component Library). Разместив компоненты, программист устанавливает их свойства и “привязывает” программные фрагменты к определенным событиям.

Библиотека Visual Component Library содержит более ста компонентов. Помимо стандартных объектов пользовательского интерфейса Microsoft Windows имеются компоненты для: наиболее употребительных элементов управления Windows 95; элементов управления, связанных с базами данных; объектов баз данных, например, таблиц и транзакций; объектов для составления отчетов; компонентов Internet. Реализована и совместимость с элементами ActiveX.

В С++ Builder применена технология инкрементного построения проекта, впервые реализованная в Delphi. Проект может быть создан в фоновом режиме, параллельно с редактированием исходного текста, что значительно сокращает время, затрачиваемое на его разработку.

Отладчик С++ Builder полностью интегрирован в пакет. При исполнении программы разработчик имеет доступ к окнам контроля значений переменных, почкам прерываний, потокам, регистрам и стекам вызовов. В любой момент программу можно приостановить, внести изменения и частично перестроить проект. Конструктор форм и другие инструментальные средства продолжают функционировать во время выполнения программы, что позволяет в ходе отладки добавлять новые события[10].

Вышеперечисленные, а также многие другие достоинства пакета Borland C++ Builder, делают его очень удобной средой для разработки программ под Windows 95 и Windows NT, что стало решающим аргументом при выборе среды программирования для написания программы анализа системного журнала безопасности.

### 6.3.3.Функции программы

Программа должна быть способна проводить анализ файла журнала безопасности и на его основе выдавать в наглядном виде следующие результаты:

* общая информация (размер файла журнала, количество записей, дата первой и последней записи и т.д.);
* диаграмма, показывающая распределение количества событий НСД для каждого пользователя;
* диаграмма, показывающая распределение количества событий НСД для каждой рабочей станции;
* график динамики событий НСД по дням в пределах месяца;
* график динамики событий НСД по часам в пределах суток.

Кроме того, программа должна позволять просто просматривать журнал безопасности и предоставлять возможность фильтрации событий по пользователям, рабочим станциям, категориям событий, периоду времени.

### 6.3.4.Разработка интерфейса программы

# ЗАКЛЮЧЕНИЕ

В данном дипломном проекте была рассмотрена проблема обеспечения безопасности информации в локальной вычислительной сети подразделения с заданной организационно-штатной структурой на базе Windows NT. Основным требованием, предъявляемым к проектируемой ЛВС, является безопасность данных.

В качестве логической структуры сети выбрана модель основного домена, как наиболее эффективная модель при имеющихся условиях.

Был проведен всесторонний анализ возможностей операционной системы Windows NT, в результате которого было установлено, что штатных средств обеспечения безопасности не достаточно. На основе предъявленных требований был сделан выбор дополнительного средства – программно-аппаратного комплекса Secret Net NT.

Рекомендуется применять совместно с программно-аппаратными и организационные меры предупреждения утечки закрытой информации. Это должно дать максимальный эффект.

При развитии системы, возможно, придется отказаться то модели основного домена, как не эффективной для сложных сетей с большим количеством машин и сильно разветвленной структурой групп пользователей. В качестве альтернативы может быть предложена модель многочисленных основных доменов, как наиболее актуальная для таких сетей.

# Список литературы

1. А.Юдин. ”Концепции и руководство по планированию Microsoft Windows NT Server”.
2. В.Мельников. ”Защита информации в компьютерных системах”. Москва. ”Финансы и статистика”. ”Электроинформ”. 1997.
3. “Руководство администратора безопасности системы “Secret Net NT”. Информзащита.
4. С.Штайнке. “Идентификация и криптография”. LAN\Журнал сетевых решений. 1998. №2.
5. В.Жельников. “Криптография от папируса до компьютера”. ABF. Москва. 1997.
6. “Руководство администратора по установке Secret Net NT”. Информзащита.
7. Б.Нанс. “Компьютерные сети”. Москва. Бином. 1996.
8. Г.Дейтел. “Введение в операционные системы”. Т.2. Москва. Мир. 1987.
9. П.Дайсон. “Овладеваем пакетом Norton Utilities 6”. Москва. Мир. 1993.
10. Д.Боулинг. “С++ в поисках RADости”. PC Magazine. 1997. №5.
11. Н.З.Елманова, С.П.Кошель. “Введение в Borland C++ Builder”. Москва. Диалог-МИФИ. 1998.

# Приложение 1

**Список наиболее частых паролей**

aaa

abc

afgan

alex

alexey

andrei

andrey

ann

anton

apple

band

bank

baron

bear

beat

beatles

best

beta

black

blue

board

boris

boy

can

castle

cat

center

chance

chaos

cherry

club

computer

cross

data

death

december

delta

denis

devil

dima

dmitry

dmitriy

dog

door

dragon

dream

eagle

east

easy

elena

eugene

eye

field

filter

finish

flower

force

friend

fun

george

girl

golf

great

green

gray

hand

hell

hello

help

hero

hockey

horse

house

igor

ilya

info

irene

iron

jazz

job

julia

jury

killer

kirill

knight

kostya

land

larry

last

legal

lenin

light

little

long

lord

love

mad

magic

major

mark

market

master

moscow music

natalia

network

nice

night

normal

north

old

oleg

omega

panel

paradise

password

pavel

peter

philip

phone

pilot

pizza

police

prince

protect

quest

rain

ranger

real

red

remote

risk

river

robot

roman

room

rose

ruslan

russia

sasha

school

secret

secure

serge

sergei

sergey

service

sex

shadow

shark

shit

shop

simple

sky

slava

simple

sound

south

spy

square

standard

star

station

street

success

summer

super

sweet

system

target

team

tiger

time

toy

trade

true

unknown

victor

visit

vlad

vladimir

water

west

white

yuri

zone