**Безопасность компьютерных сетей в банке**

***Классификация сетей.***

Сети компьютеров имеют множество преимуществ перед совокупностью отдельных систем, в их числе следующие:

\* Разделение ресурсов.

Пользователи сети могут иметь доступ к определенным ресурсам всех узлов сети. В их числе, например, наборы данных, свободная память на удаленных узлах, вычислительная мощность удаленных процессоров и т.д. Это позволяет экономить значительные средства за счет оптимизации использования ресурсов и их динамического перераспределения в процессе работы.

\* Повышение надежности функционирования системы. Поскольку сеть состоит из совокупности отдельных узлов, то в случае сбоя на одном или нескольких узлах другие узлы смогут взять на себя их функции. При этом пользователи могут даже и не заметить этого- перераспределение задач возьмет на себя программное обеспечение сети.

\* Распределение загрузки.

В сетях с переменным уровнем загруженности имеется возможность перераспределять задачи с одних узлов сети (с повышенной нагрузкой) на другие, где имеются свободные ресурсы. Такое перераспределение может производиться динамически в процессе работы, более того, пользователи могут даже и не знать об особенностях планирования задач в сети. Эти функции может брать на себя программное обеспечение сети.

\* Расширяемость.

Сеть может быть легко расширена за счет добавления новых узлов. При этом архитектура практически всех сетей позволяет легко адаптировать сетевое программное обеспечение к изменениям конфигурации. Более того, это может производиться автоматически.

Однако с точки зрения безопасности эти достоинства превращаются в уязвимые места, порождая серьезные проблемы.

Особенности работы в сети определяются ее двойственным характером: с одной стороны, сеть следует рассматривать как единую систему, а с другой, - как совокупность независимых систем, каждая из которых выполняет свои функции; имеет своих пользователей. Эта же двойственность проявляется в логическом и физическом восприятии сети: на физическом уровне взаимодействие отдельных узлов осуществляется с помощью сообщений различного вида и формата, которые интерпретируются протоколами. На логическом уровне (т.е. сточки зрения протоколов верхних уровней) сеть представляется как совокупность функций, распределенных по различным узлам, но связанных в единый комплекс.

Сети подразделяются: [8, с.4-7]

1 По топологии сети (классификация по организации физического уровня).

\* Общая шина.

Все узлы соединены с общей высокоскоростной шиной передачи данных. Они одновременно настроены на прием сообщения, но каждый узел может принять только то сообщение, которое предназначено ему. Адрес идентифицируется контроллером сети, при этом в сети может быть только один узел с заданным адресом. Если два узла одновременно заняты передачей сообщения (столкновение пакетов), то один из них или они оба ее прекращают, ожидают случайный интервал времени, затем возобновляют попытку передачи (метод разрешения конфликтов). Возможен другой случай — в момент передачи каким-либо узлом сообщения по сети, другие узлы начать передачу не могут (метод предотвращения конфликтов). Такая топология сети является очень удобной: все узлы являются равноправными, логическое расстояние между любыми двумя узлами равно 1, скорость передачи сообщений велика. Впервые организация сети «общая шина» и соответствующие протоколы нижних уровней были разработаны совместно компаниями DIGITAL и Rank Xerox, она получила название Ethernet.

\* Кольцо.

Сеть построена в виде замкнутого контура однонаправленных каналов между станциями. Каждая станция принимает сообщения по входному каналу, в начале сообщения содержится адресная и управляющая информация. На основании ее станция принимает решение сделать копию сообщения и убрать его из кольца либо передать по выходному каналу на соседний узел. Если в настоящий момент не передается никакого сообщения, станция сама может передать сообщение.

В кольцевых сетях используется несколько различных способов управления:

- гирляндная — управляющая информация передается по отдельным совокупностям (цепям) компьютеров кольца;

- управляющий маркер — управляющая информация оформляется в виде определенного битового шаблона, циркулирующего по кольцу; только при получении маркера станция может выдать сообщение в сеть (наиболее известный способ, получивший название token ring);

- сегментная — по кольцу циркулирует последовательность сегментов. Обнаружив пустой, станция может поместить в него сообщение и передать в сеть;

- вставка регистров — сообщение загружается в регистр сдвига и передается в сеть когда кольцо свободно.

\* Звезда.

Сеть состоит из одного узла-концентратора и нескольких соединенных с ним терминальных узлов, непосредственно между собой несвязанных. Один или несколько терминальных узлов могут являться концентраторами другой сети, в этом случае сеть приобретает древовидную топологию.

Управление сетью полностью осуществляется концентратором; терминальные узлы могут связываться между собой только через него. Обычно на терминальных узлах выполняется лишь локальная обработка данных. Обработка данных, имеющих отношение ко всей сети, осуществляется на концентраторе. Она носит название централизованной. Управление сетью обычно осуществляется с помощью процедуры опроса: концентратор через определенные промежутки времени опрашивает по очереди терминальные станции - есть ли для него сообщение. Если есть - терминальная станция передает сообщение на концентратор, если нет - осуществляется опрос следующей станции. Концентратор может передать сообщение одному или нескольким терминальным станциям в любой момент времени.

2. По размерам сети:

\* Локальные. Сеть передачи данных, связывающая ряд узлов в одной локальной зоне (комната, организация); обычно узлы сети комплектуются однотипным аппаратным и программным обеспечением (хотя это и необязательно). Локальные сети обеспечивают высокие скорости передачи информации. Локальные сети характеризуются короткими (не более нескольких километров) линиями связи, контролируемой рабочей средой, низкой вероятностью ошибок, упрощенными протоколами. Для связи локальных сетей с территориальными используются шлюзы.

\* Территориальные. Отличаются от локальных большей протяженностью линий связи (город, область, страна, группа стран), которые могут обеспечиваться телекоммуникационными компаниями. Территориальная сеть может связывать несколько локальных сетей, отдельные удаленные терминалы и ЭВМ и может быть соединена с другими территориальными сетями.

Территориальные сети редко используют какие-либо типовые топологические конструкции, так как они предназначены для выполнения других, обычно специфических задач. Поэтому они как правило строятся в соответствии с произвольной топологией, управление осуществляется с помощью специфических протоколов.

3. По организации обработки информации (классификация на логическом уровне представления; здесь под системой понимается вся сеть как единый комплекс):

\* Централизованная.

Системы такой организации наиболее широко распространены и привычны. Они состоят из центрального узла, реализующего весь комплекс выполняемых системой функций, и терминалов, роль которых сводится к частичному вводу и выводу информации. В основном периферийные устройства играют роль терминалов, с которых осуществляется управление процессом обработки информации. Роль терминалов могут выполнять дисплейные станции или персональные компьютеры, как локальные, так и удаленные. Любая обработка (в том числе связь с другими сетями) выполняется через центральный узел. Особенностью таких систем является высокая нагрузка на центральный узел, в силу чего там должен быть высоконадежный и высокопроизводительный компьютер. Центральный узел является наиболее уязвимой частью системы: выход его из строя выводит из строя всю сеть. В тоже время задачи обеспечения безопасности в централизованных системах решаются наиболее просто и фактически сводятся к защите центрального узла.

Другой особенностью таких систем является неэффективное использование ресурсов центрального узла, а также неспособность гибкой перестройки характера работы (центральный компьютер должен работать все время, а значит какую-то его часть он может работать вхолостую). В настоящее время доля систем с централизованным управлением постепенно падает.

\* Распределенная.

Практически все узлы этой системы могут выполнять сходные функции, причем каждый отдельный узел может использовать оборудование и программное обеспечение других узлов. Основной частью такой системы является распределенная ОС, которая распределяет объекты системы: файлы, процессы (или задачи), сегменты памяти, другие ресурсы. Но при этом ОС может распределять не все ресурсы или задачи, а только часть их, например, файлы и свободную память на диске. В этом случае система все равно считается распределенной, количество ее объектов (функций, которые могут быть распределены по отдельным узлам) называется степенью распределенности. Такие системы могут быть как локальными, так и территориальными. Говоря математическим языком, основной функцией распределенной системы является отображение отдельных задач во множество узлов, на которых происходит их выполнение [7, с.49]. Распределенная система должна обладать следующими свойствами: [11]

1. Прозрачностью, то есть система должна обеспечить обработку информации вне зависимости от ее местонахождения.

2. Механизмом распределения ресурсов, который должен выполнять следующие функции: обеспечивать взаимодействие процессов и удаленный вызов задач, поддерживать виртуальные каналы, распределенные транзакции и службу имен.

3. Службой имен, единой для всей системы, включая поддержку единой службы директорий.

4. Реализацией служб гомогенных и гетерогенных сетей.

5. Контролем функционирования параллельных процессов.

6. Безопасностью. В распределенных системах проблема безопасности переходит на качественно новый уровень, поскольку приходится контролировать ресурсы и процессы всей системы в целом, а также передачу информации между элементами системы. Основные составляющие защиты остаются теми же - контроль доступа и информационных потоков, контроль трафика сети, аутентификация, операторский контроль и управление защитой. Однако контроль в этом случае усложняется.

Распределенная система обладает рядом преимуществ, не присущих никакой другой организации обработки информации: оптимальностью использования ресурсов, устойчивостью к отказам (выход из строя одного узла не приводит к фатальным последствиям - его легко можно заменить) и т.д. Однако при этом возникают новые проблемы: методика распределения ресурсов, обеспечение безопасности, прозрачности и др. В настоящее время все возможности распределенных систем реализованы далеко не полностью.

В последнее время все большее признание получает концепция обработки информации клиент-сервер. Данная концепция является переходной от централизованной к распределенной и одновременно объединяющей обе последних. Однако клиент-сервер - это не столько способ организации сети, сколько способ логического представления и обработки информации.

Клиент-сервер - это такая организация обработки информации, при которой все выполняемые функции делятся на два класса: внешние и внутренние. Внешние функции состоят из поддержки интерфейса пользователя и функций представления информации на уровне пользователя. Внутренние касаются выполнения различных запросов, процесса обработки информации, сортировки и др.

Сущность концепции клиент-сервер заключается в том, что в системе выделяются элементы двух уровней: серверы, выполняющие обработку данных (внутренние функции), и рабочие станции, выполняющие функции формирования запросов и отображения результатов их обработки (внешние функции). От рабочих станций к серверу идет поток запросов, в обратном направлении - результаты их обработки. Серверов в системе может быть несколько и они могут выполнять различные наборы функций нижнего уровня (серверы печати, файловые и сетевые серверы). Основной объем информации обрабатывается на серверах, которые в этом случае играют роль локальных центров; информация вводится и выводится с помощью рабочих станций.

Отличительные особенности систем, построенных по принципу клиент-сервер, следующие:

- наиболее оптимальное использование ресурсов;

- частичное распределение процесса обработки информации в сети;

- прозрачный доступ к удаленным ресурсам;

- упрощенное управление;

- пониженный трафик;

- возможность более надежной и простой защиты;

- большая гибкость в использовании системы в целом, а также разнородного оборудования и программного обеспечения;

- централизованный доступ к определенным ресурсам,

Отдельные части одной системы могут строится по различным принципам и объединяться с использованием соответствующих согласующих модулей. Каждый класс сетей имеет свои специфические особенности как в плане организации, так и в плане защиты.

***Обеспечение безопасности сетей.***

Как уже отмечалось выше, несомненные преимущества обработки информации в сетях ЭВМ оборачиваются немалыми сложностями при организации их защиты. Отметим следующие основные проблемы:

\* Разделение совместно используемых ресурсов.

В силу совместного использования большого количества ресурсов различными пользователями сети, возможно находящимися на большом расстоянии друг от друга, сильно повышается риск НСД - в сети его можно осуществить проще и незаметнее.

\* Расширение зоны контроля.

Администратор или оператор отдельной системы или подсети должен контролировать деятельность пользователей, находящихся вне пределов его досягаемости, возможно, в другой стране. При этом он должен поддерживать рабочий контакт со своими коллегами в других организациях.

\* Комбинация различных программно-аппаратных средств.

Соединение нескольких систем, пусть даже однородных по характеристикам, в сеть увеличивает уязвимость всей системы в целом. Система настроена на выполнение своих специфических требований безопасности, которые могут оказаться несовместимы с требованиями на других системах. В случае соединения разнородных систем риск повышается.

\* Неизвестный периметр.

Легкая расширяемость сетей ведет к тому, что определить границы сети подчас бывает сложно; один и тот же узел может быть доступен для пользователей различных сетей. Более того, для многих из них не всегда можно точно определить сколько пользователей имеют доступ к определенному узлу и кто они.

\* Множество точек атаки.

В сетях один и тот же набор данных или сообщение могут передаваться через несколько промежуточных узлов, каждый из которых является потенциальным источником угрозы. Естественно, это не может способствовать повышению защищенности сети. Кроме того, ко многим современным сетям можно получить доступ с помощью коммутируемых линий связи и модема, что во много раз увеличивает количество возможных точек атаки. Такой способ прост, легко осуществим и трудно контролируем; поэтому он считается одним из наиболее опасных. В списке уязвимых мест сети также фигурируют линии связи и различные виды коммуникационного оборудования: усилители сигнала, ретрансляторы, модемы и т.д.

\* Сложность управления и контроля доступа к системе.

Многие атаки на сеть могут осуществляться без получения физического доступа к определенному узлу - с помощью сети из удаленных точек. В этом случае идентификация нарушителя может оказаться очень сложной, если не невозможной. Кроме того, время атаки может оказаться слишком мало для принятия адекватных мер.

По своей сути проблемы защиты сетей обусловлены двойственным характером последних: об этом мы говорили выше. С одной стороны, сеть есть единая система с едиными правилами обработки информации, а с другой, - совокупность обособленных систем, каждая из которых имеет свои собственные правила обработки информации. В частности, эта двойственность относится и к проблемам защиты. Атака на сеть может осуществляться с двух уровней (возможна их комбинация):

1. Верхнего - злоумышленник использует свойства сети для проникновения на другой узел и выполнения определенных несанкционированных действий. Предпринимаемые меры защиты определяются потенциальными возможностями злоумышленника и надежностью средств защиты отдельных узлов.

2. Нижнего - злоумышленник использует свойства сетевых протоколов для нарушения конфиденциальности или целостности отдельных сообщений или потока в целом. Нарушение потока сообщений может привести к утечке информации и даже потере контроля за сетью. Используемые протоколы должны обеспечивать защиту сообщений и их потока в целом.

Защита сетей, как и защита отдельных систем, преследует три цели: поддержание конфиденциальности передаваемой и обрабатываемой в сети информации, целостности и доступности ресурсов и компонентов сети.

Эти цели определяют действия по организации защиты от нападений с верхнего уровня. Конкретные задачи, встающие при организации защиты сети, обуславливаются возможностями протоколов высокого уровня: чем шире эти возможности, тем больше задач приходится решать. Действительно, если возможности сети ограничиваются пересылкой наборов данных, то основная проблема защиты заключается в предотвращении НСД к наборам данных, доступным для пересылки. Если же возможности сети позволяют организовать удаленный запуск программ, работу в режиме виртуального терминала, то необходимо реализовывать полный комплекс защитных мер.

Как и для АСОИБ, защита сети должна планироваться как единый комплекс мер, охватывающий все особенности обработки информации. В этом смысле организация защиты сети, разработка политики безопасности, ее реализация и управление защитой подчиняются общим правилам, которые были рассмотрены выше. Однако необходимо учитывать, что каждый узел сети должен иметь индивидуальную защиту в зависимости от выполняемых функций и от возможностей сети. При этом защита отдельного узла должна являться частью общей защиты. На каждом отдельном узле необходимо организовать:

- контроль доступа ко всем файлам и другим наборам данных, доступным из локальной сети и других сетей;

- контроль процессов, активизированных с удаленных узлов;

- контроль сетевого графика;

- эффективную идентификацию и аутентификацию пользователей, получающих доступ к данному узлу из сети;

- контроль доступа к ресурсам локального узла, доступным для использования пользователями сети;

- контроль за распространением информации в пределах локальной сети и связанных с нею других сетей.

Однако сеть имеет сложную структуру: для передачи информации с одного узла на другой последняя проходит несколько стадий преобразований. Естественно, все эти преобразования должны вносить свой вклад в защиту передаваемой информации, в противном случае нападения с нижнего уровня могут поставить под угрозу защиту сети. Таким образом, защита сети как единой системы складывается из мер защиты каждого отдельного узла и функций защиты протоколов данной сети.

Необходимость функций защиты протоколов передачи данных опять же обуславливается двойственным характером сети: она представляет собой совокупность обособленных систем, обменивающихся между собой информацией с помощью сообщений. На пути от одной системы к другой эти сообщения преобразуются протоколами всех уровней. А поскольку они являются наиболее уязвимым элементом сети, протоколы должны предусматривать обеспечение их безопасности для поддержки конфиденциальности, целостности и доступности информации, передаваемой в сети.

Сетевое программное обеспечение должно входить в состав сетевого узла, в противном случае возможно нарушение работы сети и ее защиты путем изменения программ или данных. При этом протоколы должны реализовывать требования по обеспечению безопасности передаваемой информации, которые являются частью общей политики безопасности. Ниже приводится классификация угроз, специфических для сетей (угрозы нижнего уровня):

1. Пассивные угрозы (нарушение конфиденциальности данных, циркулирующих в сети) — просмотр и/или запись данных, передаваемых по линиям связи:

- просмотр сообщения - злоумышленник может просматривать содержание сообщения, передаваемого по сети;

- анализ графика - злоумышленник может просматривать заголовки пакетов, циркулирующих в сети и на основе содержащейся в них служебной информации делать заключения об отправителях и получателях пакета и условиях передачи (время отправления, класс сообщения, категория безопасности и т.д.); кроме того, он может выяснить длину сообщения и объем графика.

2. Активные угрозы (нарушение целостности или доступности ресурсов сети) — несанкционированное использование устройств, имеющих доступ к сети для изменения отдельных сообщений или потока сообщений:

- отказ служб передачи сообщений - злоумышленник может уничтожать или задерживать отдельные сообщения или весь поток сообщений;

- «маскарад» — злоумышленник может присвоить своему узлу или ретранслятору чужой идентификатор и получать или отправлять сообщения от чужого имени;

- внедрение сетевых вирусов — передача по сети тела вируса с его последующей активизацией пользователем удаленного или локального узла;

- модификация потока сообщений — злоумышленник может выборочно уничтожать, модифицировать, задерживать, переупорядочивать и дублировать сообщения, а также вставлять поддельные сообщения.

Совершенно очевидно, что любые описанные выше манипуляции с отдельными сообщениями и потоком в целом, могут привести к нарушениям работы сети или утечке конфиденциальной информации. Особенно это касается служебных сообщений, несущих информацию о состоянии сети или отдельных узлов, о происходящих на отдельных узлах событиях (удаленном запуске программ, например) — активные атаки на такие сообщения могут привести к потере контроля за сетью. Поэтому протоколы, формирующие сообщения и ставящие их в поток, должны предпринимать меры для их защиты и неискаженной доставки получателю.

Решаемые протоколами задачи аналогичны задачам, решаемым при защите локальных систем: обеспечение конфиденциальности обрабатываемой и передаваемой в сети информации, целостности и доступности ресурсов (компонентов) сети. Реализация этих функций осуществляется с помощью специальных механизмов. К их числу следует отнести:

- Механизмы шифрования, которые обеспечивают конфиденциальность передаваемых данных и/или информации о потоках данных. Используемый в данном механизме алгоритм шифрования может использовать секретный или открытый ключ. В первом случае предполагается наличие механизмов управления и распределения ключей. Различают два способа шифрования: канальное, реализуемое с помощью протокола канального уровня, и оконечное (абонентское), реализуемое с помощью протокола прикладного или, в некоторых случаях, представительного уровня.

В случае канального шифрования защищается вся передаваемая по каналу связи информация, включая служебную. Этот способ имеет следующие особенности:

- вскрытие ключа шифрования для одного канала не приводит к компрометации информации в других каналах;

- вся передаваемая информация, включая служебные сообщения, служебные поля сообщений с данными, надежно защищена;

- вся информация оказывается открытой на промежуточных узлах -ретрансляторах, шлюзах и т.д.;

- пользователь не принимает участия в выполняемых операциях;

- для каждой пары узлов требуется свой ключ;

- алгоритм шифрования должен быть достаточно стоек и обеспечивать скорость шифрования на уровне пропускной способности канала (иначе возникнет задержка сообщений, которая может привести к блокировке системы или существенному снижению ее производительности);

- предыдущая особенность приводит к необходимости реализации алгоритма шифрования аппаратными средствами, что увеличивает расходы на создание и обслуживание системы.

Оконечное (абонентское) шифрование позволяет обеспечивать конфиденциальность данных, передаваемых между двумя прикладными объектами. Другими словами, отправитель зашифровывает данные, получатель - расшифровывает. Такой способ имеет следующие особенности (сравните с канальным шифрованием):

- защищенным оказывается только содержание сообщения; вся служебная информация остается открытой;

- никто кроме отправителя и получателя восстановить информацию не может (если используемый алгоритм шифрования достаточно стоек);

- маршрут передачи несущественен — в любом канале информация останется защищенной;

- для каждой пары пользователей требуется уникальный ключ;

- пользователь должен знать процедуры шифрования и распределения ключей.

Выбор того или иного способа шифрования или их комбинации зависит от результатов анализа риска. Вопрос стоит следующим образом: что более уязвимо — непосредственно отдельный канал связи или содержание сообщения, передаваемое по различным каналам. Канальное шифрование быстрее (применяются другие, более быстрые, алгоритмы), прозрачно для пользователя, требует меньше ключей. Оконечное шифрование более гибко, может использоваться выборочно, однако требует участия пользователя. В каждом конкретном случае вопрос должен решаться индивидуально.

- Механизмы цифровой подписи, которые включают процедуры закрытия блоков данных и проверки закрытого блока данных. Первый процесс использует секретную ключевую информацию, второй — открытую, не позволяющую восстановить секретные данные. С помощью секретной информации отправитель формирует служебный блок данных (например, на основе односторонней функции), получатель на основе общедоступной информации проверяет принятый блок и определяет подлинность отправителя. Сформировать подлинный блок может только пользователь, имеющий соответствующий ключ.

\* Механизмы контроля доступа.

Осуществляют проверку полномочий сетевого объекта на доступ к ресурсам. Проверка полномочий производится в соответствии с правилами разработанной политики безопасности (избирательной, полномочной или любой другой) и реализующих ее механизмов.

\* Механизмы обеспечения целостности передаваемых данных.

Эти механизмы обеспечивают как целостность отдельного блока или поля данных, так и потока данных. Целостность блока данных обеспечивается передающим и принимающим объектами. Передающий объект добавляет к блоку данных признак, значение которого является функцией от самих данных. Принимающий объект также вычисляет эту функцию и сравнивает ее с полученной. В случае несовпадения выносится решение о нарушении целостности. Обнаружение изменений может повлечь за собой действия по восстановлению данных. В случае умышленного нарушения целостности может быть соответствующим образом изменено и значение контрольного признака (если алгоритм его формирования известен), в этом случае получатель не сможет установить нарушение целостности. Тогда необходимо использовать алгоритм формирования контрольного признака как функцию данных и секретного ключа. В этом случае правильное изменение контрольного признака без знания ключа будет невозможно и получатель сможет установить, подвергались ли данные модификации.

Защита целостности потоков данных (от переупорядочивания, добавления, повторов или удаления сообщений) осуществляется с использованием дополнительных формы нумерации (контроль номеров сообщений в потоке), меток времени и т.д.

Желательными компонентами защиты сети являются следующие механизмы: [8, с.34]

\* Механизмы аутентификации объектов сети.

Для обеспечения аутентификации используются пароли, проверка характеристик объекта, криптографические методы (аналогичные цифровой подписи). Эти механизмы обычно применяются для аутентификации одноуровневых сетевых объектов. Используемые методы могут совмещаться с процедурой «троекратного рукопожатия» (троекратный обмен сообщениями между отправителем и получателем с параметрами аутентификации и подтверждениями).

\* Механизмы заполнения текста.

Используются для обеспечения защиты от анализа графика. В качестве такого механизма может использоваться, например, генерация фиктивных сообщений (богусов); в этом случае трафик имеет постоянную интенсивность во времени.

\* Механизмы управления маршрутом.

Маршруты могут выбираться динамически или быть заранее заданы с тем, чтобы использовать физически безопасные подсети, ретрансляторы, каналы. Оконечные системы при установлении попыток навязывания могут потребовать установления соединения по другому маршруту. Кроме того, может использоваться выборочная маршрутизация (то есть часть маршрута задается отправителем явно - в обход опасных участков).

\* Механизмы освидетельствования.

Характеристики данных, передаваемые между двумя и более объектами (целостность, источник, время, получатель) могут подтверждаться с помощью механизма освидетельствования. Подтверждение обеспечивается третьей стороной (арбитром), которой доверяют все заинтересованные стороны и которая обладает необходимой информацией.

Помимо перечисленных выше механизмов защиты, реализуемых протоколами различных уровней, существует еще два, не относящихся к определенному уровню. Они по своему назначению аналогичны механизмам контроля в локальных системах:

\* Обнаружение и обработка событий (аналог средств контроля опасных событий).

Предназначены для обнаружения событий, которые приводят или могут привести к нарушению политики безопасности сети. Список этих событий соответствует списку для отдельных систем. Кроме того, в него могут быть включены события, свидетельствующие о нарушениях в работе перечисленных выше механизмов защиты. Предпринимаемые в этой ситуации действия могут включать различные процедуры восстановления, регистрацию событий, одностороннее разъединение, местный или периферийный отчет о событии (запись в журнал) и т.д.

\* Отчет о проверке безопасности (аналог проверки с использованием системного журнала).

Проверка безопасности представляет собой независимую проверку системных записей и деятельности на соответствие заданной политике безопасности.

Функции защиты протоколов каждого уровня определяются их назначением:

1. Физический уровень - контроль электромагнитных излучений линий связи и устройств, поддержка коммуникационного оборудования в рабочем состоянии. Защита на данном уровне обеспечивается с помощью экранирующих устройств, генераторов помех, средств физической защиты передающей среды.

2. Канальный уровень - увеличение надежности защиты (при необходимости) с помощью шифрования передаваемых по каналу данных. В этом случае шифруются все передаваемые данные, включая служебную информации.

3. Сетевой уровень - наиболее уязвимый уровень с точки зрения защиты. На нем формируется вся маршрутизирующая информация, отправитель и получатель фигурируют явно, осуществляется управление потоком. Кроме того, протоколами сетевого уровня пакеты обрабатываются на всех маршрутизаторах, шлюзах и др. промежуточных узлах. Почти все специфические сетевые нарушения осуществляются с использованием протоколов данного уровня (чтение, модификация, уничтожение, дублирование, переориентация отдельных сообщений или потока в целом, маскировка под другой узел и др.).

Защита от всех подобных угроз осуществляется протоколами сетевого и транспортного уровней и с помощью средств криптозащиты. На данном уровне может быть реализована, например, выборочная маршрутизация.

4. Транспортный уровень - осуществляет контроль за функциями сетевого уровня на приемном и передающем узлах (на промежуточных узлах протокол транспортного уровня не функционирует). Механизмы транспортного уровня проверяют целостность отдельных пакетов данных, последовательности пакетов, пройденный маршрут, время отправления и доставки, идентификацию и аутентификацию отправителя и получателя и др. функции. Все активные угрозы становятся видимыми на данном уровне.

Гарантом целостности передаваемых данных является криптозащита данных и служебной информации. Никто кроме имеющих секретный ключ получателя и/или отправителя не может прочитать или изменить информацию таким образом, чтобы изменение осталось незамеченным.

Анализ графика предотвращается передачей сообщений, не содержащих информацию, которые, однако, выглядят как настоящие. Регулируя интенсивность этих сообщений в зависимости от объема передаваемой информации можно постоянно добиваться равномерного графика. Однако все эти меры не могут предотвратить угрозу уничтожения, переориентации или задержки сообщения. Единственной защитой от таких нарушений может быть параллельная доставка дубликатов сообщения по другим путям.

5. Протоколы верхних уровней обеспечивают контроль взаимодействия принятой или переданной информации с локальной системой. Протоколы сеансового и представительного уровня функций защиты не выполняют. В функции защиты протокола прикладного уровня входит управление доступом к определенным наборам данных, идентификация и аутентификация определенных пользователей, а также другие функции, определяемые конкретным протоколом. Более сложными эти функции являются в случае реализации полномочной политики безопасности в сети.