The slide features several decorative circles in a light purple color. One circle is empty and located on the left side. Another empty circle is at the top left, partially overlapping the main title. Two solid purple circles are at the top right, also overlapping the main title. A solid purple circle is at the bottom left. A solid purple circle is at the bottom center, overlapping the subtitle. An empty circle is at the bottom right, also overlapping the subtitle.

# Информационная безопасность

Защита информации в  
вычислительных сетях

# Вычислительные сети



- Современная информационная система, как правило, функционирует в режиме распределенной обработки данных. Она включает в себя различные вычислительные системы, которые соединяются между собой вычислительной сетью.
- Обмен информацией в сети происходит между:
  - Пользователями;
  - Процессами разных элементов сети;
  - Между пользователями и процессами.

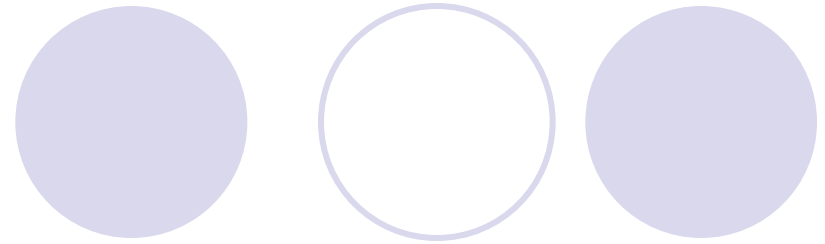
# Обмен информацией в сети

- При обмене информацией в сети соблюдаются следующие положения:
  - Каждый пользователь и процесс имеет свой уровень полномочий;
  - Проходящая транзитом через узел коммутации абонентская информация должна быть не видимой для персонала данного узла;
  - Транзитная абонентская информация не должна подвергаться документированию в узле;
  - Транзитная абонентская информация при обработке в узле не должна запоминаться в долговременной памяти.

# Особенности современных информационных систем

- С точки зрения информационной безопасности наиболее существенными являются следующие аспекты:
  - Корпоративная сеть является распределенной, связи между отдельными частями обеспечиваются внешними провайдерами
  - Корпоративная сеть имеет одно или несколько подключений к Internet
  - Критически важные серверы могут располагаться на различных площадках
  - Для доступа пользователей используются как компьютеры так и другие мобильные устройства
  - В течение одного сеанса работы пользователь обращается к нескольким информационным сервисам
  - Требования доступности информационных сервисов выдвигаются достаточно жесткие
  - Информационная система представляет собой сеть с активными агентами, в процессе работы программные модули передаются с сервера на компьютеры пользователя и т.п.
  - Не все пользовательские системы контролируются администраторами ИС
  - Программное обеспечение и модули полученные по сети не могут рассматриваться как надежные
  - Конфигурация ИС постоянно изменяется на уровнях администрирования данных, программ, аппаратуры

# Модель OSI



- При рассмотрении процедур межсетевого взаимодействия всегда опираются на стандарты, разработанные *International Standard Organization (ISO)*.
- Эти стандарты получили название "Семиуровневой модели сетевого обмена" или в английском варианте "*Open System Interconnection Reference Model*" (*OSI Ref.Model*).
- В данной модели обмен информацией может быть представлен в виде стека, представленного на рисунке.



# Применение модели OSI



- На базе этой модели описываются правила и процедуры передачи данных, а также структуры открытых систем и комплексы стандартов, которым должны удовлетворять системы. Основными элементами модели являются уровни, объекты соединения и физические средства соединений.
- **Физические средства соединения** – совокупность физической среды, аппаратных и программных средств, обеспечивающая передачу сигнала.

# Физический уровень



- Физический уровень определяет механические, оптические, электрические, процедурные средства передачи сигналов через физические соединения.
- Основная задача – создание физических интерфейсов для подключения к физическим средствам соединения.
- Функции физического уровня:
  - Установление и разъединение физических соединений;
  - Передача последовательности сигналов;
  - Прослушивание канала;
  - Выполнение идентификации канала;
  - Оповещение о неисправностях и отказах.

# Канальный уровень



- Канал – средство (маршрут), по которому передаются данные.
- По одному физическому каналу взаимодействуют группа пар систем.
- Маршрут по которому передаются данные от источника к адресату называется **логическим каналом**;
- Канал, проходящий через всю коммуникационную сеть, именуется **виртуальным каналом**.
- Канальный уровень – осуществляет формирование и передачу блоков данных между системами.
- Функции канального уровня:
  - Организация канальных соединений и идентификация их портов;
  - Организация последовательности блоков данных;
  - Обнаружение и исправление ошибок;
  - Передача блоков данных;
  - Управление потоками данных;
  - Обеспечение прозрачности логических каналов.



# Сетевой уровень



- Сетевой уровень обеспечивает прокладку каналов, соединяющих абонентские системы и системы управления через коммуникационные каналы. Задача данного уровня создание виртуальных каналов. Передача данных осуществляется пакетами, в которых помещаются фрагменты данных.
- Функции сетевого уровня:
  - Создание сетевых соединений и идентификация их портов;
  - Обнаружение и исправление ошибок;
  - Управление потоками данных;
  - Организация последовательности пакетов;
  - Маршрутизация и коммутация;
  - Сегментирование и объединение пакетов;
  - Возврат в исходное состояние.

# Транспортный уровень



- Транспортный уровень определяет адресацию абонентских систем в информационной сети. Данный уровень обеспечивает передачу пакетов через коммуникационную сеть, используя виртуальные каналы.
- Функции транспортного уровня:
  - Управление передачей блоков данных и обеспечение их целостности;
  - Обнаружение ошибок, сообщение о неисправленных ошибках;
  - Восстановление передачи после отказов;
  - Изменение размера блоков данных;
  - Предоставление приоритетов при передаче блоков данных;
  - Передача подтверждений о передаче данных;
  - Ликвидация блоков при тупиковых ситуациях в сети.

# Сеансовый уровень



- Сеанс – цикл операций, выполняемый без перерыва и обеспечивающий взаимодействие между участниками.
- Процедуры, выполняемые для проведения сеанса: установление сеанса, идентификация сеанса, восстановление сеанса после отказа, сбоя или ошибки, прекращение сеанса.
- Функции сеансового уровня:
  - Установление и завершение на сеансовом уровне соединения;
  - Выполнение нормального и срочного обмена данными между прикладными процессами;
  - Управление взаимодействием прикладных процессов;
  - Синхронизация работы сеансовых соединений;
  - Извещение прикладных процессов об исключительных ситуациях;
  - Установление меток в прикладных процессах;
  - Прерывание прикладного процесса и его корректное возобновление;
  - Прекращение сеанса без потери данных.

# Представительный уровень

- Представительный уровень описывает в нужной форме данные, передаваемые между прикладными процессами. Данный уровень обеспечивает работу с синтаксисом данных, определяя структуру команд, сообщений и ответов.
- Основные функции:
  - Генерация запросов на установление сеансов взаимодействия прикладных процессов;
  - Согласование между прикладными процессами видов представления данных;
  - Реализация форм представления данных;
  - Представление графических материалов;
  - Обеспечение конфиденциальности данных;
  - Передача запросов на прекращение сеанса.

# Прикладной уровень



- Прикладной процесс обеспечивает обработку данных для нужд пользователя.
- Прикладной уровень обеспечивает прикладные процессы средствами доступа к области взаимодействия.
- Функции прикладного уровня:
  - Описание форм и методов взаимодействия прикладных процессов;
  - Выполнение различных видов операций с данными;
  - Идентификация пользователей;
  - Определение функционирующих абонентов;
  - Объявление о возможности доступа к прикладным процессам;
  - Определение достаточности ресурсов;
  - Посылка запросов на соединение с другими пользователями;
  - подача заявок уровню представлений на необходимые методы описания информации;
  - Синхронизация взаимодействия прикладных процессов;
  - Определение качества обслуживания;
  - Соглашение об исправлении ошибок и определении достоверности данных.

# Потенциальные угрозы безопасности информации в ЛВС

- Доступ в ЛВС со стороны штатного компьютера;
- Доступ со стороны кабельных линий связи:
  - Со стороны штатного пользователя нарушителя;
  - При подключении постороннего компьютера и другой аппаратуры;
  - При побочных электромагнитных излучениях и наводках информации;
- Аварийная ситуация, отказ аппаратуры, ошибки операторов и разработчиков программного обеспечения и т.п.

# Классификация сетевых атак

- При описании сетевых атак в общем случае используется следующее представление:
  - существует информационный поток от отправителя (файл, пользователь, компьютер) к получателю (файл, пользователь, компьютер):



# Сетевые атаки

- **I. Пассивная атака**
- Пассивной называется такая *атака*, при которой *противник* не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью *пассивной атаки* может быть только прослушивание передаваемых сообщений и анализ трафика.





# Сетевые атаки

- Активной называется такая *атака*, при которой *противник* имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Различают следующие типы *активных атак*:
- **Отказ в обслуживании - DoS-атака (Denial of Service)**
  - Отказ в обслуживании нарушает нормальное функционирование сетевых сервисов. *Противник* может перехватывать все сообщения, направляемые определенному адресату. Другим примером подобной *атаки* является создание значительного трафика, в результате чего сетевой сервис не сможет обрабатывать запросы законных клиентов.
  - Классическим примером такой *атаки* в сетях TCP/IP является SYN-атака, при которой нарушитель посылает пакеты, инициирующие установление TCP-соединения, но не посылает пакеты, завершающие установление этого соединения.
  - В результате может произойти переполнение памяти на сервере, и серверу не удастся установить соединение с законными пользователями.



# Сетевые атаки

- **Модификация потока данных** - атака "*man in the middle*"
- Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.



# Сетевые атаки

- **Создание ложного потока (фальсификация)**
- *Фальсификация* (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого



# Сетевые атаки

- **Повторное использование**
- Повторное использование означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа - это так называемая *replay-атака*.
- На самом деле *replay-атаки* являются одним из вариантов фальсификации, но в силу того, что это один из наиболее распространенных вариантов *атаки* для получения несанкционированного доступа, его часто рассматривают как отдельный тип *атаки*.



# Функции межсетевых экранов

- В межсетевом экране может быть реализовано несколько видов защиты. К их числу относятся:
  - фильтрация сетевых пакетов
  - средства идентификации и аутентификации пользователей
  - средства оповещения и сигнализации о выявленных нарушениях
  - другие.

# Фильтрация сетевого трафика

- Фильтрация входящей и исходящей информации осуществляется на основе правил в нескольких уровнях.
- На основе транспортных адресов отправителя и получателя производится фильтрация соединений на сетевом и транспортном уровне. Одновременно осуществляется контроль доступа в соответствии с установленными правилами разграничения доступа к сетевым ресурсам и сервисам.
- Второй этап фильтрации выполняется на уровне приложений. Для этого создаются специальные фильтры прикладного уровня, каждый из которых отвечает за фильтрацию информационного обмена по одному отдельному протоколу и между одним определенным типом приложений. На этом уровне обрабатываются протоколы HTTP, FTP, SMTP, TELNET и SNMP.
- С целью увеличения пропускной способности межсетевого экрана (а он рассчитан на работу в высокоскоростных сетях пропускной способностью до 100 Мб) могут быть созданы шлюзы приложений на уровне ядра операционной системы. Их основная задача - пропустить протокол, который они обслуживают, через МЭ на уровне пакетного фильтра, что позволяет существенно повысить быстродействие МЭ. Через такие шлюзы пропускают данные для приложений, работающих по FTP, Rlogin/Rsh и RealAudio.

# Необходимость механизмов защиты

- Сообщение, которое передается от одного участника другому, проходит через различного рода сети. При этом будем считать, что устанавливается логический информационный канал от отправителя к получателю с использованием различных коммуникационных протоколов (например, TCP/IP).
- Средства безопасности необходимы, если требуется защитить передаваемую информацию от *противника*, который может представлять угрозу *конфиденциальности, аутентификации, целостности* и т.п. Все технологии повышения безопасности имеют два компонента:
  - Относительно безопасная передача информации. Примером является вид шифрования, когда сообщение изменяется таким образом, что становится нечитаемым для *противника*, и, возможно, дополняется кодом, который основан на содержимом сообщения и может использоваться для *аутентификации* отправителя и обеспечения *целостности* сообщения.
  - Некоторая секретная информация, разделяемая обоими участниками и неизвестная *противнику*. Примером является ключ шифрования.
  - Кроме того, в некоторых случаях для обеспечения безопасной передачи бывает необходима *третья доверенная сторона* (third trusted party - ТТР). Например, *третья сторона* может быть ответственной за распределение между двумя участниками секретной информации, которая не стала бы доступна *противнику*. Либо *третья сторона* может использоваться для решения споров между двумя участниками относительно достоверности передаваемого сообщения.

# Шифрование данных

- В дополнение к базовой модели взаимодействия открытых систем ISO выдала рекомендации по созданию сервисных служб защиты, функции которых должны реализовываться при помощи восьми процедур защиты.
- **Шифрование данных** используется:
  - Для закрытия всех данных абонента;
  - Для закрытия некоторых полей сообщения.
- Выделяют следующие уровни шифрования:
  - Шифрование в канале связи (весь поток);
  - Межконцевое (абонентское) шифрование.



# Цифровая подпись



- **Цифровая подпись** служит для подтверждения подлинности отправителя сообщения (удостоверяется факт о том, что источником сообщения является указанный в заголовке абонент).

# Управление доступом к ресурсам сети

- Управление доступом к ресурсам сети выполняется на основании множества правил и формальных моделей, которые имеют различные аргументы:
  - Идентификаторы абонентов;
  - Информация о ресурсах;
  - Списки разрешенных операций;
  - Временные ограничения и т.д.

# Обеспечение целостности данных

- Обеспечение целостности данных – дополнительная информация, которая является функцией от содержания сообщения и вводится в передаваемое сообщение. Имеется два типа:
  - Средство обеспечивает целостность отдельного блока данных;
  - Средство обеспечивает целостность потока блоков данных или отдельных полей этих блоков.

# Процедуры аутентификации

- **Процедуры аутентификации** – необходимы для защиты при передаче в сети паролей, аутентификаторов логических объектов и .т.д
- Цель – защита от установления с объектом, образованным нарушителей и действующим под его управлением с целью имитации работы подлинного объекта.

# Процедура заполнения потока

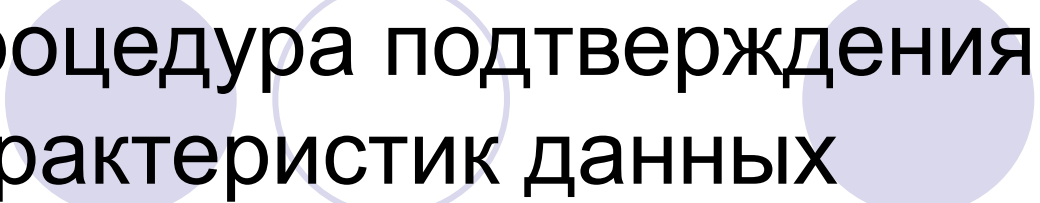
- **Процедура заполнения потока** – предотвращает возможность анализа трафика. Эффективность повышается, если одновременно применяется линейное шифрование потока данных.

# Управление маршрутом



- Управление маршрутом движения данных используется для организации передачи данных только по маршрутам, образованным с помощью надежных и безопасных устройств и систем.

# Процедура подтверждения характеристик данных



- Процедура подтверждения характеристик данных предполагает наличие арбитра (третьей доверенной стороны).
- Функция арбитра – подтвердить подлинность абонентов, целостность и время передачи сообщения.

# Модель сетевого взаимодействия

- Модель безопасного сетевого взаимодействия в общем виде можно представить следующим образом:

