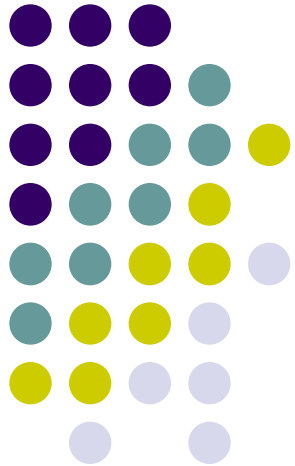
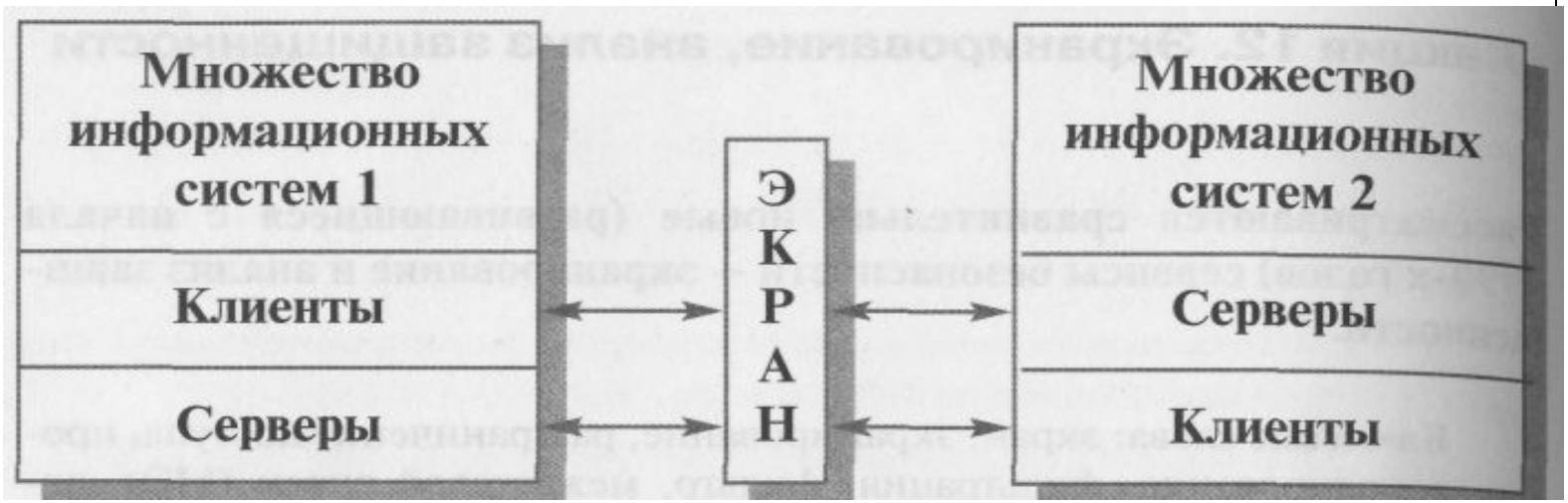
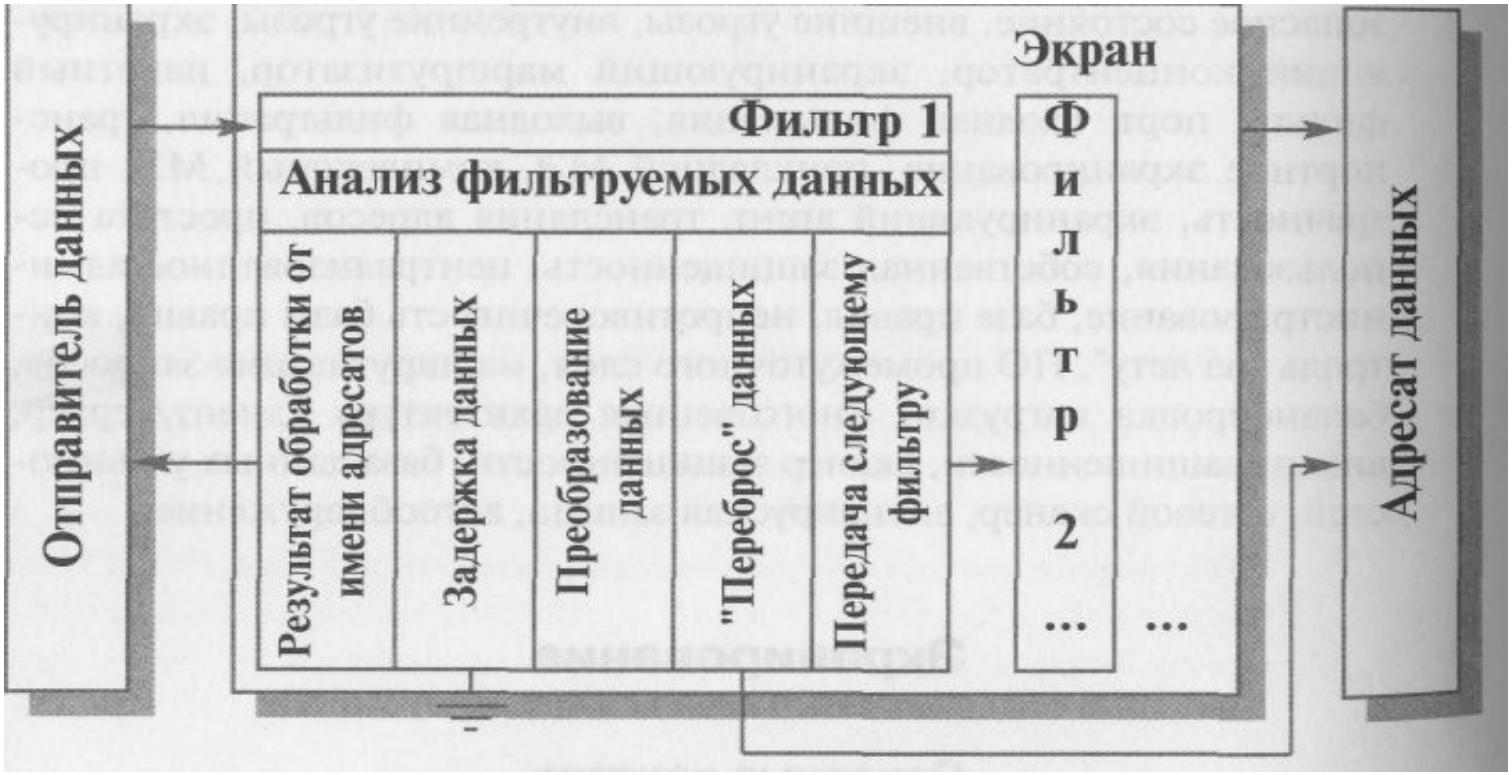
Экранирование, анализ защищенности



Формальная постановка задачи экранирования



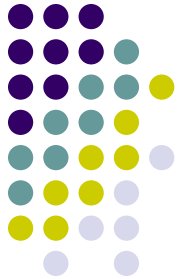
- Пусть имеется два множества информационных систем.
- Экран — это средство разграничения доступа клиентов из одного множества к серверам из другого множества.
- Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем



Экран удобно представлять как **последовательность фильтров**.

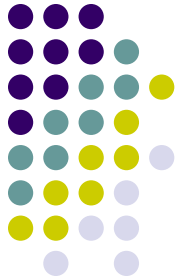
- Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран.
- **Допускается**
  - преобразование данных,
  - передача порции данных на следующий фильтр для продолжения анализа
  - обработка данных от имени адресата и возврат результата отправителю
- Экраны также осуществляют **протоколирование** обмена информацией.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи".



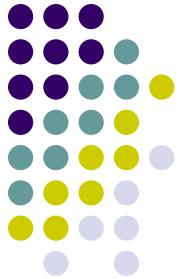
- **Задача экранирования - защита внутренней области от потенциально враждебной внешней.**
- Межсетевые экраны (МЭ) **firewall** чаще всего устанавливают для защиты корпоративной сети организации, имеющей выход в Internet

Экранирование позволяет

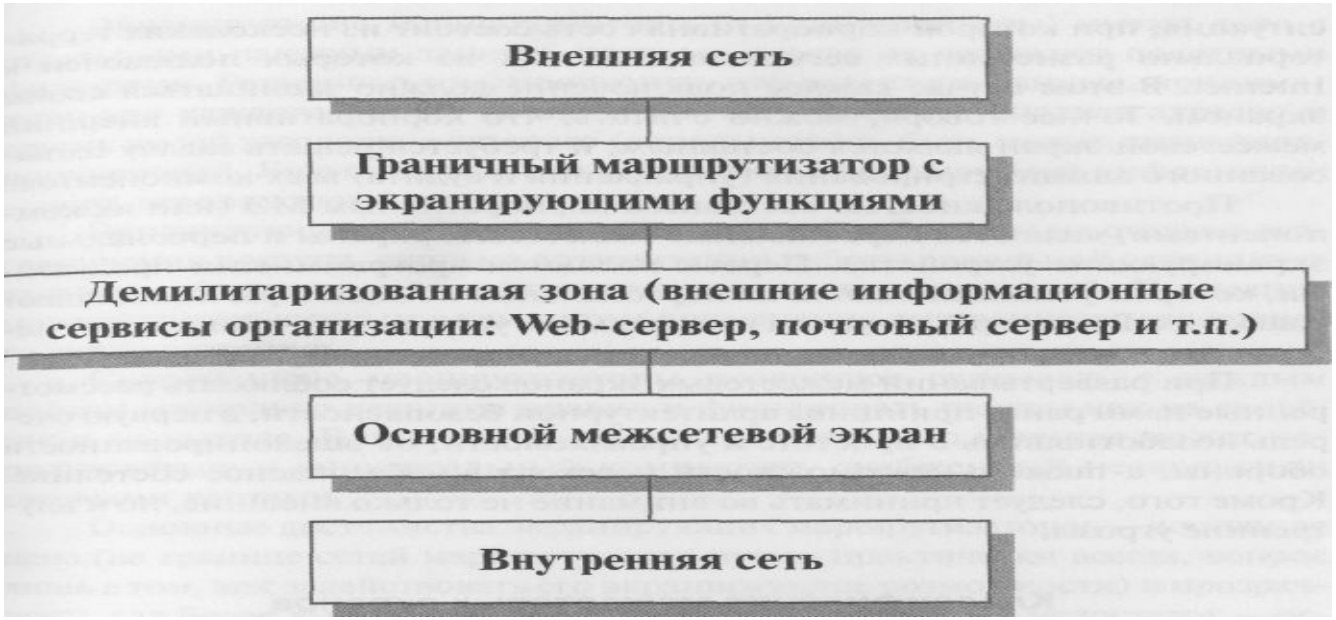


- Поддерживать доступность сервисов внутренней области, уменьшая нагрузку, вызванную внешней активностью.
- Уменьшить уязвимость внутренних сервисов безопасности,.
- Экранирующая система, в отличие от универсальной, может быть устроена более простым более безопасным образом.
- Контролировать информационные потоки, направленные во внешнюю область, что способствует поддержанию режима **конфиденциальности** в ИС организации.

Архитектурные аспекты



- Межсетевой экран располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети).
- Межсетевой экран - идеальное место для встраивания средств активного аудита.
- На межсетевой экран целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

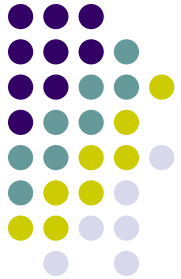


- для защиты внешних подключений обычно используется **двухкомпонентное экранирование**
- **граничным маршрутизатором** ,за которым располагается так называемая **демилитаризованная зона** (сеть с умеренным доверием безопасности, куда выносятся внешние информационные сервисы организации — Web, электронная почта и т.п.) и
- **основной МЭ**, защищающий внутреннюю часть корпоративной сети.

Персональные межсетевые экраны и персональные экранирующие устройства

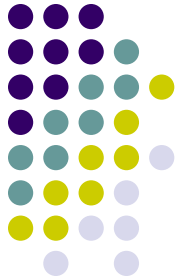
- **Персональные межсетевые экраны** являются программными продуктами, которые устанавливаются на персональные компьютеры и защищают только их.
- **Персональные экранирующие устройства** реализуются на отдельных устройствах и защищают небольшую локальную сеть, такую как сеть домашнего офиса.

Принципы архитектурной безопасности



- простота и управляемость,
- эшелонированность обороны,
- о невозможность перехода в небезопасное состояние.
- принимать во внимание не только внешние, но и внутренние угрозы.

Классификация межсетевых экранов



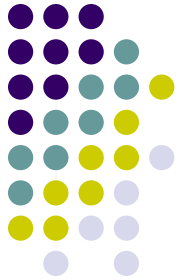
При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI.

Межсетевые экраны также целесообразно классифицировать **по уровню фильтрации** — канальному, сетевому, транспортному или прикладному.

1. экранирующие концентраторы (мостах, коммутаторах) (уровень 2),
2. маршрутизаторы(уровень 3),
3. о транспортном экранировании (уровень 4)
4. и о прикладныеэкраны (уровень 7).

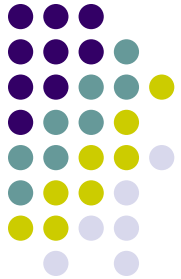
Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

Экранирующие маршрутизаторы и концентраторы (пакетные фильтры)



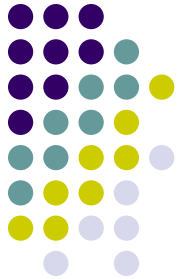
- имеют дело с отдельными пакетами данных
- Решения о том, пропустить или задержать данные, принимаются **для каждого пакета независимо**, на основании анализа
  - адресов и других полей заголовков сетевого (канального) и, быть может, транспортного уровней.
  - порт, через который поступил пакет.
- Экранирующие **концентраторы являются средством** не столько разграничения доступа, сколько **оптимизации работы локальной сети** за счет организации так называемых виртуальных локальных сетей, являющихся результатом применения внутреннего межсетевого экранирования.
- Современные маршрутизаторы позволяют связывать с каждым портом несколько десятков правил и **фильтровать пакеты как на входе, так и на выходе.**

Основные достоинства и недостатки



- **Основные достоинства** экранирующих маршрутизаторов –
  - доступная цена и
  - прозрачность для более высоких уровней модели OSI.
- **Основной недостаток** —
  - ограниченность анализируемой информации и, как следствие,
  - относительная слабость обеспечиваемой защиты.

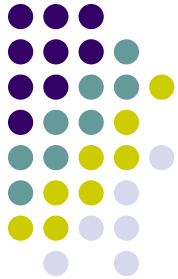
Транспортное экранирование



Позволяет контролировать процесс установления виртуальных соединений и передачу информации по ним.

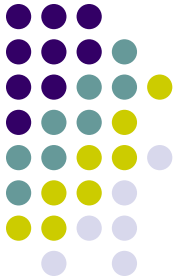
- С точки зрения реализации экранирующий транспорт представляет собой довольно простую, а значит, надежную программу.
- По сравнению с пакетными фильтрами, транспортное экранирование обладает большей информацией, поэтому соответствующий МЭ может осуществлять более тонкий контроль за виртуальными соединениями
- Главный недостаток — сужение области применения, поскольку вне контроля остаются датаграммные протоколы.
- Обычно транспортное экранирование применяют в сочетании с другими подходами, как важный дополнительный элемент.

Прикладное экранирование



- Межсетевой экран, функционирующий на прикладном уровне, способен обеспечить **наиболее надежную защиту**.
- Как правило, подобный Э представляет собой универсальный компьютер, на котором функционируют- экранирующие агенты, интерпретирующие протоколы прикладного уровня (HTTP, FTP, SMTP, telnet и т.д.) в той степени, которая необходима для обеспечения безопасности.
- При использовании прикладных МЭ
  - **Субъекты из внешней сети видят только шлюзовой компьютер**; соответственно, им доступна только та информация о внутренней сети, которую он считает нужным экспортировать.
  - **Субъектам внутренней сети кажется, что они напрямую общаются с объектами внешнего мира.**
- **Недостаток** прикладных МЭ — отсутствие полной прозрачности, требующее специальных действий для поддержки каждого прикладного протокола.

Комплексные межсетевые экраны

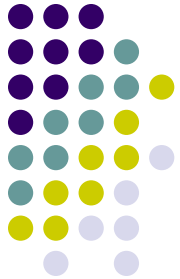


Комплексные межсетевые экраны, охватывают уровни от сетевого до прикладного.

- Защитные функции выполняются комплексными МЭ прозрачным для приложений образом, не требуя внесения изменений ни в существующее программное обеспечение, ни в привычные действия пользователей.
- **Комплексность МЭ может достигаться разными способами**:
  - "снизу вверх", от сетевого уровня через накопление контекста к прикладному уровню
  - "сверху вниз", посредством дополнения прикладного МЭ механизмами транспортного и сетевого уровней.
- Помимо выразительных возможностей и допустимого количества правил, **качество межсетевого экрана** определяется еще двумя очень важными характеристиками —
  - **простотой использования и**
  - **собственной защищенностью**.

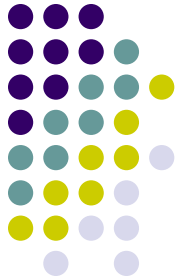
- **В плане простоты использования первостепенное значение имеют наглядный интерфейс при определении правил фильтрации** и возможность централизованного администрирования составных конфигураций.

Собственная защищенность межсетевого экрана



- обеспечивается теми же средствами, что и защищенность универсальных систем.
- физическая защита,
- идентификация и аутентификация,
- разграничение доступа,
- контроль целостности,
- протоколирование и аудит.
- защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность.
- оперативное наложение заплат, ликвидирующих выявленные уязвимые места МЭ.

Анализ защищенности



Сервис анализа защищенности предназначен для выявления уязвимых мест с целью их оперативной ликвидации.

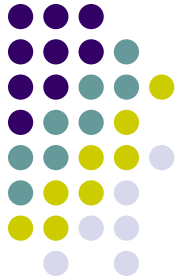
- помогает обнаружить (и устранить) пробелы в защите раньше, чем их сможет использовать злоумышленник.
- В первую очередь, имеются в виду "оперативные" бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.
- **Ядром таких систем является база уязвимых мест**, которая определяет доступный диапазон возможностей и требует практически постоянной актуализации.

Выявляются бреши

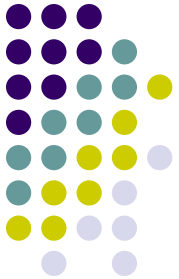
- наличие вредоносного ПО (в частности, вирусов),
- слабые пароли пользователей,
- неудачно сконфигурированные операционные системы,
- небезопасные сетевые сервисы,
- неустановленные заплаты,
- уязвимости в приложениях и т.д.

Однако наиболее эффективными являются сетевые сканеры а также антивирусные средства.

Сканеры могут выявлять уязвимые места



- **путем пассивного анализа**, то есть изучения конфигурационных файлов, задействованных портов и т.п.,
- **путем имитации действий атакующего**.
- Некоторые найденные **уязвимые места могут устраняться автоматически** (например, лечение зараженных файлов), о других сообщается администратору.



- Подавляющее большинство атак носит рутинный характер;
- они возможны только потому, что известные бреши в защите годами остаются неустраненными.
- Сервис анализа защищенности является важным рубежом эшелонированной обороны