# \*Продолжение 5 лекции\*

(Межсетевой) Экран, выполняет свои функции, контролируя все информационные потоки двумя множествами информационных систем., работая как информационная мембрана. В этом смысле, экран можно представлять себе как набор фильтров, анализирующих проходящую через них информацию и на основе заложенных в них алгоритмов, принимающих решение пропустить информацию или отказать в её пересылке. Такая система может выполнять регистрацию событий, связанных с процессами разграничения доступа. В частности, фиксировать все незаконные попытки доступа к информации и сигнализировать о ситуациях, требующих немедленной реакции.

Экранирующие системы делают несимметричными. Для экранов определяются понятия «внутри» и «снаружи». Задача экрана состоит в защите внутренней сети от потенциально враждебного окружения. Важнейшим примером потенциально враждебной внешней сети является интернет.

Рассмотрим какие проблемы возникают при построении экранирующих систем.

1. Обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи;
2. Экранирующая система должна обладать мощными и гибкими средствами управления для простого и полного воплощения в жизнь политики организации, для обеспечения простой реконфигурации система при изменении структуры сети;
3. Экранирующая система должна работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий;
4. Экранирующая система должна работать эффективно и успевать обрабатывать весь входящий и исходящий трафик пиковых режимов. Это необходимо для того, чтобы firewall нельзя было «забросать» большим количеством вызовов, которые привели бы к нарушению её работы;
5. Система обеспечения безопасности должна быть сама надёжно защищена от любых несанкционированных воздействий поскольку является ключом к конфиденциальной информации в организации;
6. В идеале, если у организации имеется несколько внешних подключений в том числе и в удалённых филиалах, Система управления экранами должна иметь возможность централизовано обеспечивать для них проведение единой политики безопасности;
7. Система firewall должна иметь средства автоматизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки и в процессе их работы требуется доступ к некоторым ресурсам внутренней компьютерной сети. В этом случае система должна уметь надёжно распознавать таких пользователей и предоставлять им доступ.

**Рассмотрим два способа ограничения доступа для www серверов:**

1. Ограничить доступ по IP адресам клиентских машин;
2. Ввести идентификатор получателя с паролем для данного вида документа.

Такого род ввод ограничений стал использоваться часто, так как многие стремятся в интернет, чтобы использовать его коммуникации. С помощью таких механизмов по разграничению прав доступа удобно производить само рассылку информации на получение которой существует договор.

**Как организовывается ограничение по IP адресам:**

Доступ к приватным документам можно разрешить/запретить, используя ip адреса конкретных машин или сеток.

Ограничение по идентификатору получателя: Доступ к приватным документам можно разрешить/запретить, используя присвоенное имя и пароль конкретного пользователя.

**Защита электронной почты**

Активно используется 2 протокола (но их, естественно, гораздо больше):

PEM – стандарт интернета для защиты электронной почты с использованием открытых или симметричных ключей. Он требует жёсткой иерархии сертификационных центров для выдачи ключей

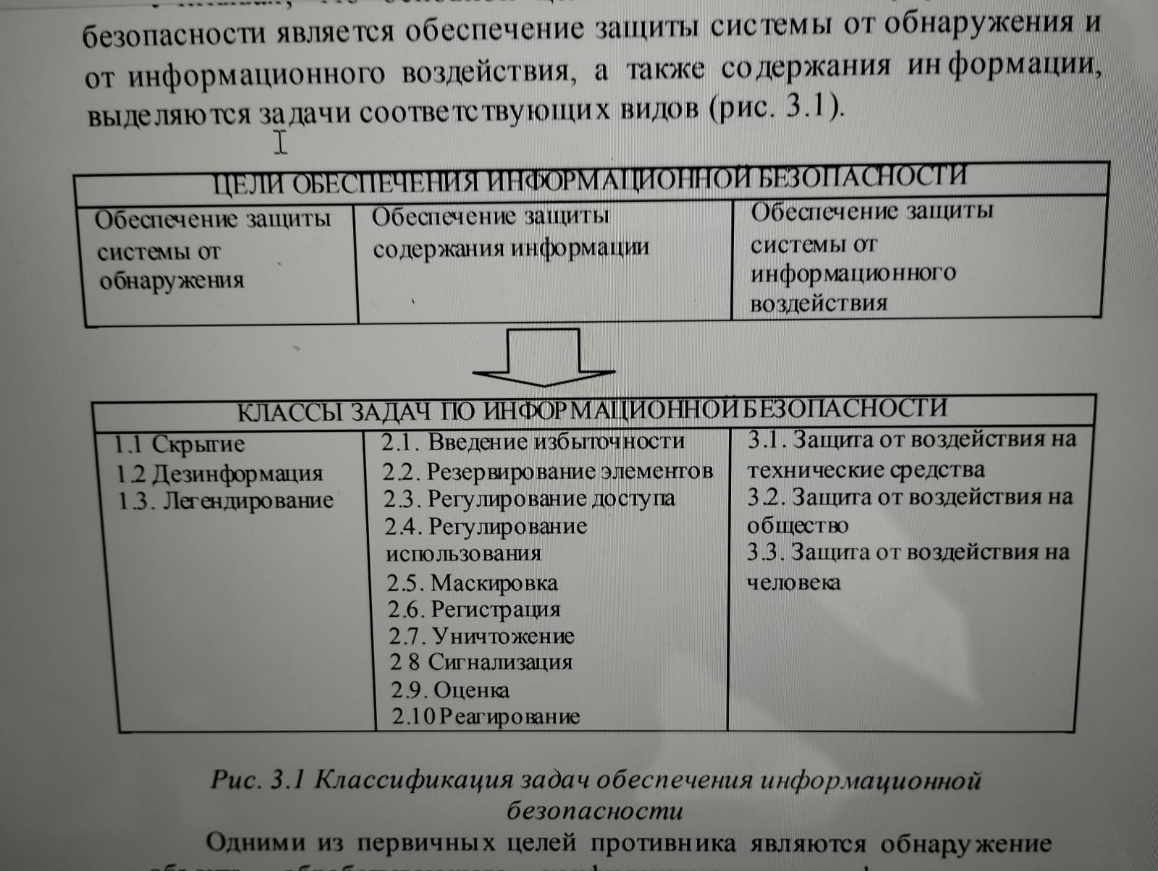
S/MIME – новый стандарт, задействует криптографические алгоритмы, использует цифровые сертификаты и, следовательно, при обеспечении аунтефикации полагается на сертификационный корпоративный центр.

Ещё одно популярное приложение PGP использует различные стандарты шифрования. Приложения шифрования/расшифровки PGP выпускаются для всех ОС.

**Цели, задачи и методы обеспечения ИБ**

Формирование множества задач осуществляется на основе анализа объективных возможностей по реализации поставленных целей защиты. Такое их множество может состоять из ряда классов.

Класс задач – это однородное в функциональном отношении множество задач, обеспечивающих полную или частичную реализацию целей.



Одними из первичных целей противника являются обнаружение объекта, обрабатывающего конфиденциальную информацию и выявление сведений о его предназначении, поэтому к первому виду задач можно отнести задачи уменьшения степени распознавания объектов. К этому виду относятся следующие виды задач – скрытие сведений о средствах, комплексов, объектов и систем обработки информации. Технические задачи направлены на устранение и ослабление демаскирующих признаков объектов защиты. При этом скрытие осуществляется уменьшением электромагнитной, временной, структурной и признаковой доступности.