Лекция 12.
Кибербезопасность в банковской области

Разработка сетевых аспектов политики безопасности

Разработка сетевых аспектов политики безопасности

- Невозможность перехода в небезопасное состояние;
- Минимизация привилегий;
- Разделение обязанностей;
- Эшелонированность обороны;

Разработка сетевых аспектов политики безопасности

- Разнообразие защитных средств;
- Простота и управляемость информационной системы;
- Обеспечение всеобщей поддержки мер безопасности.

Защита информации в электронных платежных системах

Электронная платежная система

Пластиковая карта

Банк- эмитент

Банк - эквайер

Защита информации в электронных платежных системах

Слип

Процедура авторизации

POS-терминалы (Point – of – Sale - оплата в точке продажи)

PIN - код (Personal Identification Number

Процессинговый центр

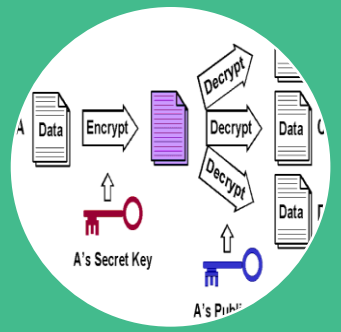
пересылка платежных и других сообщений между банком и клиентом и между банками;

обработка информации внутри организации отправителя и получателя сообщений;

доступ клиентов к средствам, аккумулированным на счетах.

SSL и SET

Протокол SSL (Secure Socket Layer)



SET (Secure Electronic Transactions)

Электронный конверт

Идентификация и проверка подлинности

Аутентификация объекта Предоставление полномочий

а) получатель должен быть уверен в подлинности источника данных;

б) получатель должен быть уверен в подлинности передаваемых данных;

в) отправитель должен быть уверен в доставке данных получателю;

г) отправитель должен быть уверен в подлинности доставленных данных;

наличие соответствующего субъекта (модуля) аутентификации;

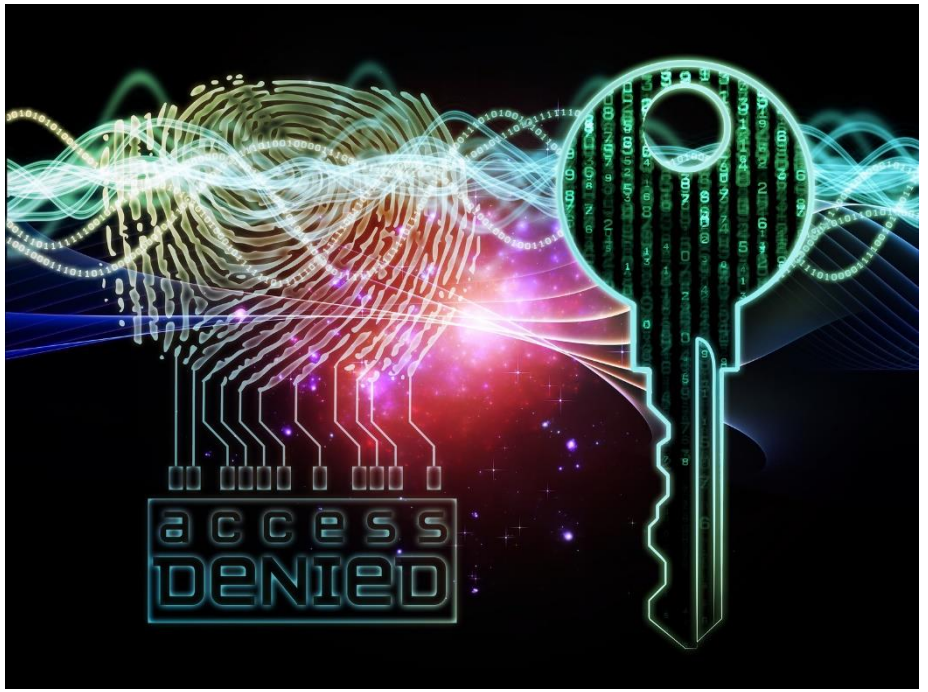
внешний аутентифицирующий объект, не принадлежащий системе;

наличие аутентифицирующего объекта, хранящего уникальную информацию для аутентификации пользователя.

внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта.

Схема простой аутентификации с помощью пароля

$$a(\mathrm{P}) = \mathrm{E}_{\mathrm{P}}(\mathrm{ID}),$$

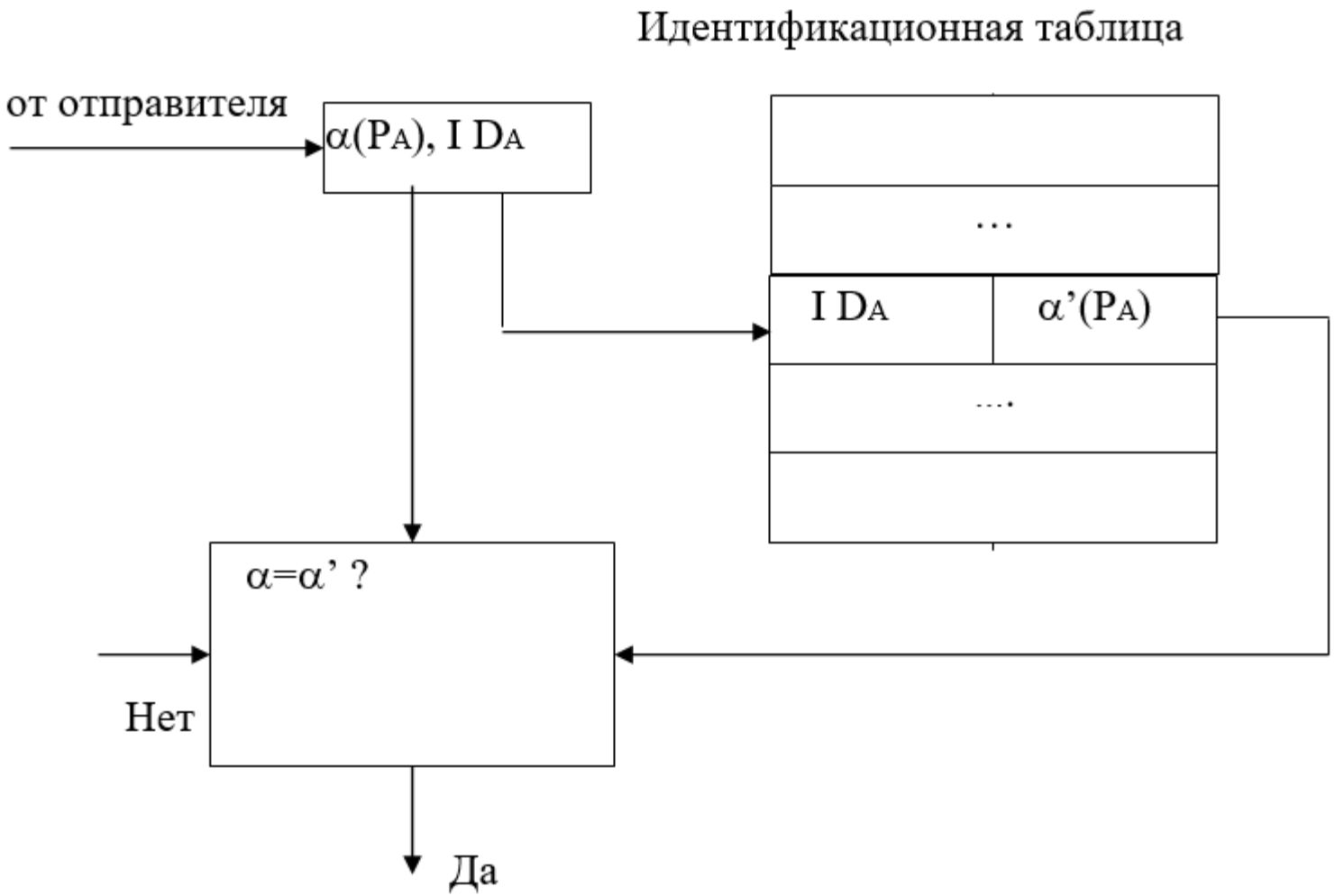


$$a(\mathrm{P}) = \mathrm{E}_{\text{РэК}}\,(\mathrm{ID}),$$

механизм запроса-ответа;

механизм отметки времени

Схема аутентификации с помощью пароля с использованием идентификационной таблицы



Электронная цифровая подпись

Электронная цифровая подпись

удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;

гарантирует целостность подписанного текста.

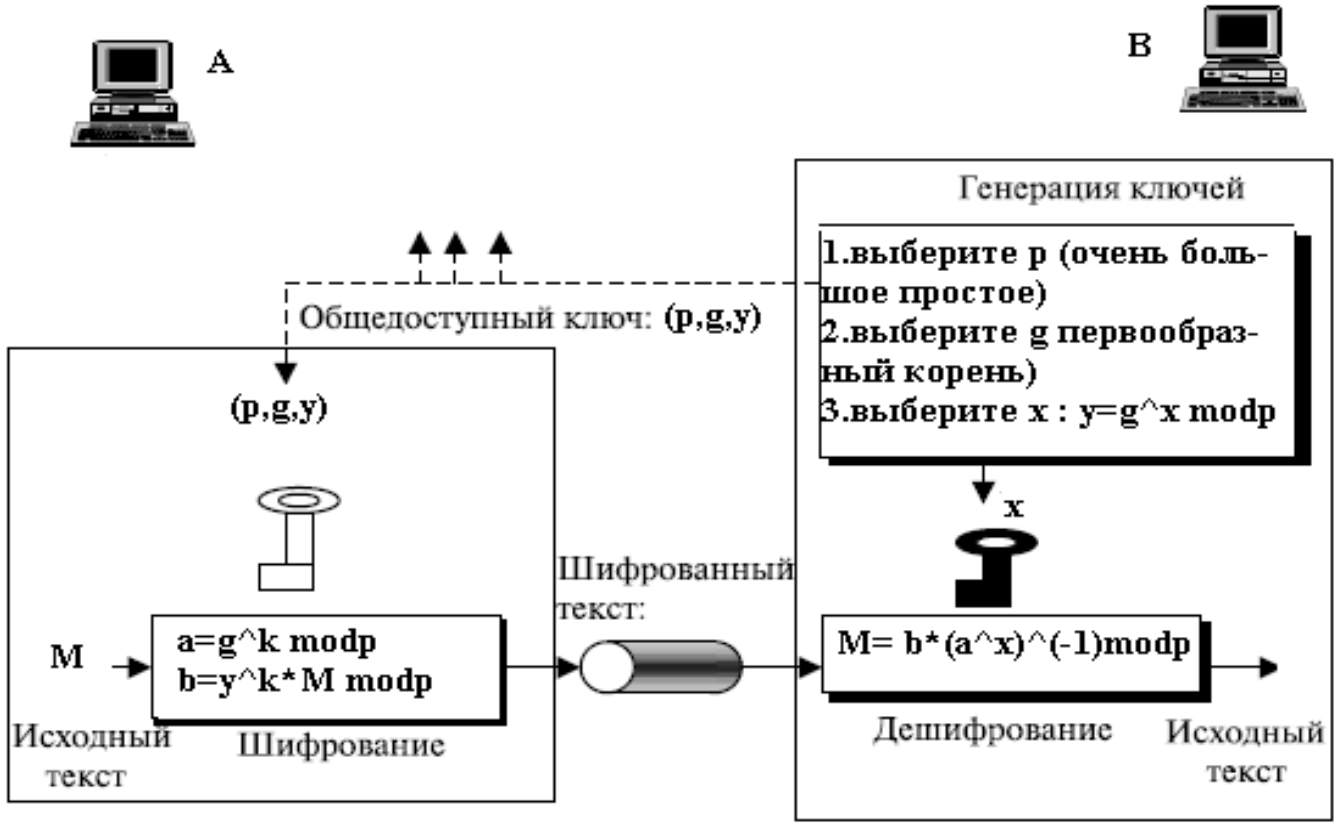
Электронная цифровая подпись

Система ЭЦП включает две процедуры:

- процедуру постановки подписи;
- процедуру проверки подписи.

- дату подписи;
- срок окончания действия ключа данной подписи;
- информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
- идентификатор подписавшего (имя открытого ключа);
- собственно цифровую подпись.

Схема цифровой подписи Эль Гамаля



Источник: https://ru.wikipedia.org/wiki/

Средства защиты от удаленных атак через сеть Интернет

защита корпоративной или локальной сети от несанкционированного удаленного доступа со стороны глобальной сети;

скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;

разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть.

межсетевой экран – фильтрующий маршрутизатор;

межсетевой экран на основе двух портового шлюза;

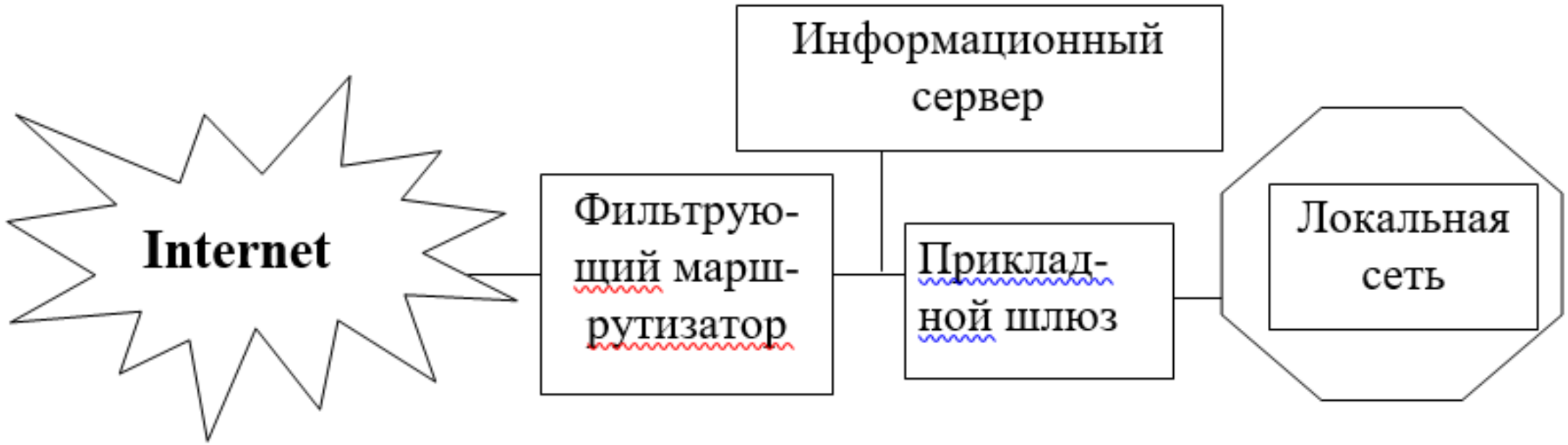
межсетевой экран на основе экранированного шлюза;

межсетевой экран – экранированная подсеть.

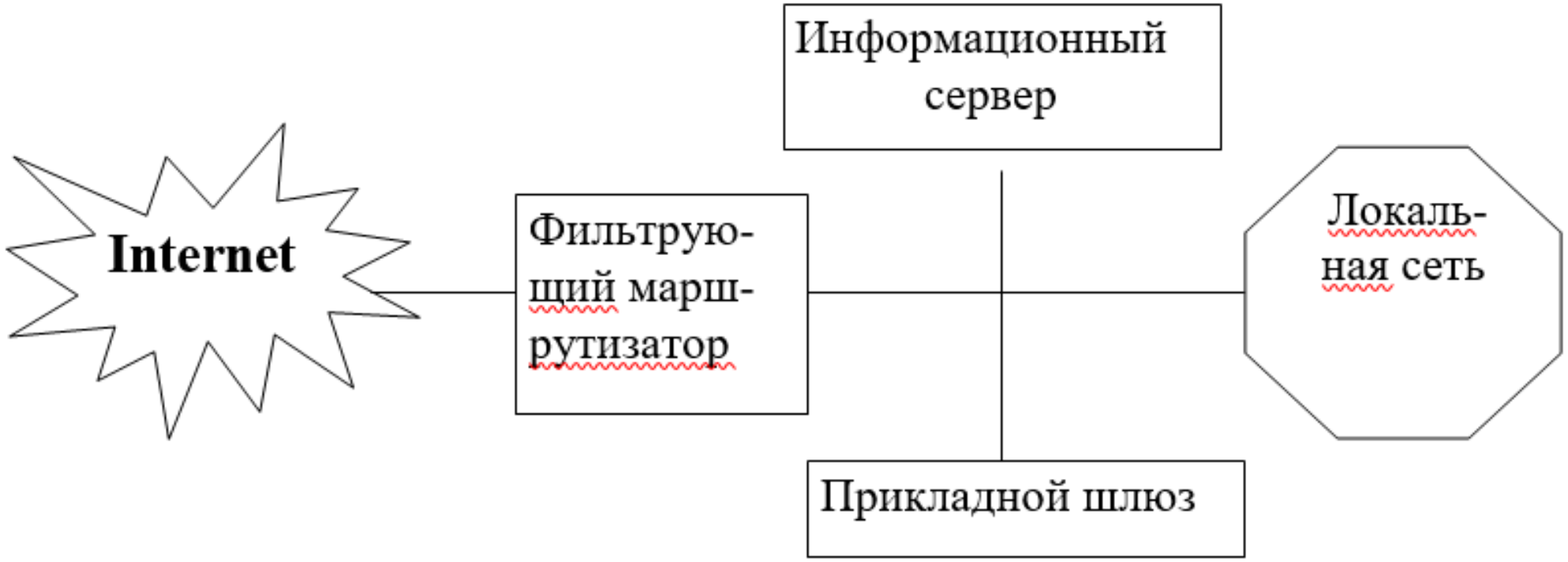
Межсетевой экран, основанный на фильтрации пакетов

- невозможность полного тестирования правил фильтрации; это приводит к незащищенности сети от не протестированных атак;
- сложность правил фильтрации, в некоторых случаях совокупность этих правил может стать неуправляемой;
- практически отсутствующие возможности регистрации событий; в результате администратору трудно определить, подвергался ли маршрутизатор атаке и скомпрометирован ли он;
- каждый хост-компьютер, связанный с сетью Internet, нуждается в своих средствах усиленной аутентификации.

Межсетевой экран с прикладным шлюзом и фильтрующим маршрутизатором



Межсетевой экран с экранированным шлюзом



- разрешается трафик от прикладного шлюза к системам сети;
- разрешается прикладной трафик от систем сети к прикладному шлюзу;
- разрешается трафик электронной почты от сервера электронной почты к системам сети;
- разрешается трафик электронной почты от систем сети к серверу электронной почты;
- разрешается трафик FTR, Gopher и т.д. от систем сети к информационному серверу;
- запрещается остальной трафик.

Спасибо за внимание