1. Перечислите три вида http-аутентификации, какие из них описаны в RFC?

**BASIC, Digest, (**Forms**), TSL**

1. Опишите схему BASIC-аутентификации.

При использовании данного вида аутентификации имя пользователя и пароль включаются в состав веб-запроса ([HTTP POST](https://ru.wikipedia.org/wiki/POST_(HTTP)) или [[GET](https://ru.wikipedia.org/wiki/HTTP#GET%7CHTTP)]). Любой перехвативший пакет легко узнает секретную информацию. Даже если контент с ограниченным доступом не слишком важен, этот метод лучше не использовать, так как пользователь может применять один и тот же пароль на нескольких [веб-сайтах](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D0%B0%D0%B9%D1%82). Также из недостатков парольной аутентификации следует отметить невысокий уровень безопасности — пароль можно подсмотреть, угадать, подобрать, сообщить посторонним лицам и т. д.

1. Опишите схему DIGEST-аутентификации.

Это аутентификация, при которой пароль пользователя передается в [хешированном](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F) виде. пароль хешируется всегда с добавлением произвольной строки символов, которая генерируется на каждое соединение заново. Таким образом при каждом соединении генерируется новый хеш пароля и перехват его ничего не даст. Дайджест-аутентификация поддерживается всеми популярными серверами и [браузерами](https://ru.wikipedia.org/wiki/%D0%91%D1%80%D0%B0%D1%83%D0%B7%D0%B5%D1%80).

1. Почему в чистом виде http-аутентификация не является надежной?

передача пароля в открытом виде