1. Перечислите все известные виды аутентификации. Какие из них описаны в RFC?

[Аутентификация по паролю1](https://habr.com/ru/companies/dataart/articles/262817/)

[Аутентификация по сертификатам1](https://habr.com/ru/companies/dataart/articles/262817/)

[Аутентификация по одноразовым паролям1](https://habr.com/ru/companies/dataart/articles/262817/)

[Аутентификация по ключам доступа1](https://habr.com/ru/companies/dataart/articles/262817/)

[Аутентификация по токенам1](https://habr.com/ru/companies/dataart/articles/262817/)

[Аутентификация по местоположению2](https://iaassaaspaas.ru/terminologiya/chto-takoe-autentifikatsiya)

[Биометрическая аутентификация3](https://community.exolve.ru/blog/authentication-vs-authorization/)

[HTTP аутентификация](https://habr.com/ru/companies/dataart/articles/262817/)[4](https://developer.mozilla.org/ru/docs/Web/HTTP/Authentication)

[Средства HTTP аутентификации, которые может использовать сервер для запроса у клиента аутентификационной информации, определены в RFC 72354](https://developer.mozilla.org/ru/docs/Web/HTTP/Authentication).

1. Опишите схему BASIC-аутентификации.

[**Схема BASIC-аутентификации:** BASIC-аутентификация - это метод, при котором username и password пользователя передаются в заголовке Authorization в незашифрованном виде (base64-encoded)1](https://habr.com/ru/companies/dataart/articles/262817/). [Обычно, клиент отображает пользователю запрос пароля, и после получения ответа отправляет запрос с пользовательскими данными в заголовке Authorization4](https://developer.mozilla.org/ru/docs/Web/HTTP/Authentication). [Обмен должен вестись через HTTPS (TLS) соединение, чтобы обеспечить защищённость4](https://developer.mozilla.org/ru/docs/Web/HTTP/Authentication).

1. Опишите схему DIGEST-аутентификации.

[**Схема DIGEST-аутентификации:** DIGEST-аутентификация - это метод, при котором сервер посылает уникальное значение nonce, а браузер передает MD5 хэш пароля пользователя, вычисленный с использованием случайных значений для затруднения криптоанализа и предотвращения replay-атак5](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%B9%D0%B4%D0%B6%D0%B5%D1%81%D1%82-%D0%B0%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F). [Этот метод предоставляет больший уровень защиты, чем базовая аутентификация5](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%B9%D0%B4%D0%B6%D0%B5%D1%81%D1%82-%D0%B0%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F).

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

[**Почему в чистом виде http-аутентификация не является надежной?** HTTP-аутентификация в чистом виде не является надежной, потому что данные отправляются в открытом виде4](https://developer.mozilla.org/ru/docs/Web/HTTP/Authentication). Это означает, что если кто-то перехватит эти данные, он сможет прочитать их без какого-либо декодирования или дешифрования. Это особенно проблематично, если данные включают конфиденциальную информацию, такую как пароли. [По этой причине, обмен должен вестись через HTTPS (TLS) соединение, чтобы обеспечить защищённость4](https://developer.mozilla.org/ru/docs/Web/HTTP/Authentication).