

**Домашнее задание № 6**

***Криптография***

Диффи Хелман, SHA, DES, SSL, TLS, HTTP/HTTPS, Certs

**1. Изучить этапы, методы и протоколы IPSec фреймворка.**

* IKE Phase 1
* IKE Phase 2
* IPSec framework protocols
* HTTP vs HTTPS

**2. SSH Best Practice.**

* На VM Uubuntu настроить SSH по лучшим практикам
* Сгенерировать на Windows host либо Kali linux VM (ssh-keygen) приватный и публичный ключ, добавить ключ (замок) ssh-add либо scp на ubuntu VM где настроили ssh
* Подключиться к ubuntu VM используя приватный ключ

**3\*. WireGuard VPN.**

* Развернуть Ubuntu с двумя сетевыми интерфейсами. Один - в интернет, другой - во внутреннюю сеть, к которой у вас подключены WS и Kali. Настроить на ней возможность подключения по RDP и SSH c WS. Срок - неделя.
* Установить и настроить WireGuard VPN на Ubuntu
* Установить агент VPN Wireguard на хостовую машину
* Установить VPN соединение между хостовой машиной и Ubuntu с VPN Wireguard

Ссылки на дополнительные ресурсы

* [Что такое IPSec и как это работает](https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security)
* [Лучшие практики по настройке SSH](https://wiki.merionet.ru/articles/luchshie-praktiki-po-zashhite-ssh-podklyucheniya)
* [Установка и конфиграция Wireguard VPN Ubuntu](https://habr.com/ru/sandbox/189100/)
* [Отличие и безопаность HTTP vs HTTPS](https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/#:~:text=The%20only%20difference%20between%20the,far%20more%20secure%20than%20HTTP.)