

Вопросы по курсу  
«Технологии и принципы защиты информации в сети интернет»  
Магистратура, РКТ, 13-14 уч. год  
Лапони́на О.Р.

1. Аутентификация и обмен ключей в протоколе SSH.
2. Семейство протоколов IPSec. Протоколы AH и ESP.
3. Семейство протоколов IPSec. Аутентификация сторон и обмен ключа в протоколе IKE.
4. Классификация межсетевых экранов. Пакетные фильтры и stateful inspection межсетевые экраны.
5. Понятие DMZ. Различные топологии DMZ сетей с использованием межсетевых экранов разного типа.
6. Классификация систем обнаружения вторжений (IDS).
7. Принципы безопасного развертывания сервисов DNS. Защита транзакции с использованием HMAC (TSIG).
8. Безопасность DNS Query / Response.
9. Технологии аутентификации в веб.
10. Безопасность веб: технологии активного содержимого на стороне сервера и связанные с этим уязвимости.