Вопросы по курсу «Технологии и принципы защиты информации в сети Интернет» Магистратура, РКТ, 10-11 уч. год Лапонина О.Р.

- 1. Аутентификация и обмен ключей в протоколе SSH.
- 2. Семейство протоколов IPSec. Протоколы АН и ESP.
- 3. Семейство протоколов IPSec. Аутентификация сторон и обмен ключа в протоколе IKE.
- 4. Классификация firewall'ов. Пакетные фильтры и stateful inspection firewall'ы.
- 5. Понятие DMZ. Различные топологии DMZ сетей с использованием firewall'ов разного типа.
- 6. Классификация Intrusion Detection Systems.
- 7. Принципы безопасного развертывания сервисов DNS. Защита транзакции с использованием HMAC (TSIG).
- 8. Безопасность DNS Query / Response.
- 9. Безопасность web: технологии активного содержимого на стороне клиента и сервера и связанные с этим уязвимости.
- 10. Технологии аутентификации в web.
- 11. Прокси сервер для web на примере ModSecurity.