

Вопросы по курсу

«Технологии и принципы защиты информации в сети интернет»

Магистратура, РКТ, 15-16 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 с поддержкой и без поддержки состояния.
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 транзакций с использованием HMAC (стандарт TSIG).
8. Безопасность DNS Query / Response (стандарт DNSSEC).
9. Технологии аутентификации в веб.
10. Безопасность веб: технологии активного содержимого на стороне сервера и связанные с этим уязвимости.
11. Технологии создания единого входа, стандарт SAML.
12. Способы управления доступом, дискреционный и мандатный способы управления доступом, RBAC.