

Вопросы по курсу

«Технологии и принципы защиты информации в сети интернет»

Магистратура, РКТ, 18-19 уч. год
Лапони́на О.Р.

1. Классификация межсетевых экранов. Пакетные фильтры с поддержкой и без поддержки состояния.
2. Понятие DMZ. Различные топологии DMZ сетей с использованием межсетевых экранов разного типа.
3. Классификация систем обнаружения вторжений (IDS).
4. Семейство протоколов IPSec. Протоколы AH и ESP.
5. Семейство протоколов IPSec. Аутентификация сторон и обмен ключа в протоколе IKE.
6. Аутентификация и обмен ключей в протоколе SSH.
7. Принципы безопасного развертывания сервисов DNS. Защита транзакций с использованием HMAC (стандарт TSIG).
8. Безопасность DNS Query / Response (стандарт DNSSEC).
9. Технологии создания единого входа, стандарт SAML.
10. Способы управления доступом, дискреционный и мандатный способы управления доступом, RBAC.
11. Безопасность веб: технологии активного содержимого на стороне сервера и связанные с этим уязвимости.
12. Основные типы уязвимостей в веб-приложениях, связанные с внедрениями.
13. Основные типы уязвимостей в веб-приложениях, связанные с межсайтовым выполнением сценариев.
14. Основные возможности межсетевого экрана прикладного уровня для протокола HTTP (WAF) ModSecurity.
15. Основные превентивные технологии обеспечения безопасности веб-приложений.